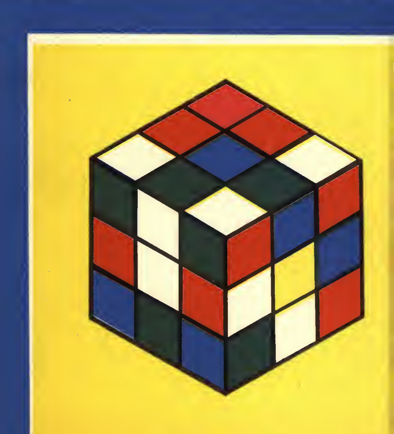
ПНТП

Л.А. КАЛУЖНИН
В.И. СУЩАНСКИЙ

ПРЕОБРАЗОВАНИЯ И ПЕРЕСТАНОВКИ



ПРОБЛЕМЫ НАУКИ
И ТЕХНИЧЕСКОГО ПРОГРЕССА

Л. А. КАЛУЖНИН, В. И. СУЩАНСКИЙ

ПРЕОБРАЗОВАНИЯ И ПЕРЕСТАНОВКИ

Перевод с украинского *Г. И. Фалина*

ИЗДАНИЕ ВТОРОЕ, ДОПОЛНЕННОЕ



МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1985

ББК 22.141
К 17
УДК 512.54+519.1+519.813

Калужнин Л. А., Сущанский В. И. Преобразования и перестановки: Пер. с укр. — 2-е изд., перераб. и доп. — М.: Наука. Главная редакция физико-математической литературы, 1985. — 160 с. — (Проблемы науки и технического прогресса).

Изучаются преобразования и перестановки конечных множеств, вводятся понятия группы перестановок и полугруппы преобразований. Приводятся элементарные сведения о группах преобразований. На конкретных примерах рассказывается о применениях теории групп при решении комбинаторных задач, изучении явлений симметрии в алгебре и геометрии, построении математической теории игр типа игры «в пятнадцать» или «кубик Рубика». Проводится математический анализ теории этих игр. Первое издание вышло в 1979 г.

Книга рассчитана на читателей, серьезно интересующихся математикой. Книга будет также интересна всем, интересующимся игрой «кубик Рубика» и другими подобными играми.

Табл. 8. Ил. 53. Библиогр. 27 назв.

Рецензент
доктор физико-математических наук *С. А. Степанов*

Лев Аркадьевич Калужнин
Виталий Иванович Сущанский

ПРЕОБАЗОВАНИЯ И ПЕРЕСТАНОВКИ

Редактор *М. М. Горячая*

Технический редактор *И. Ш. Аксельрод*

Художественный редактор *Т. Н. Кольченко*

Корректоры *Л. И. Назарова, М. Л. Медведская*

ИБ № 12670

Сдано в набор 26.11.84. Подписано к печати 31.07.85. Формат $84\times108^{1}/_{32}$. Бумага тип. № 3. Гарнитура литературная. Печать высокая. Усл. печ. л. 8,4. Усл. кр.-отт. 8,82. Уч.-изд. л. 8,73. Тираж 143 000 экз. Заказ № 860. Цена 55 коп.

Ордена Трудового Красного Знамени издательство «Наука»
Главная редакция физико-математической литературы
117071 Москва В-71, Ленинский проспект, 15

Ордена Трудового Красного Знамени Первая типография издательства «Наука». 199034, Ленинград, В-34, 9 линия, 12

К $\frac{1702030000-121}{053(02)-85}$ 180-85

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

В книге в популярной форме излагаются начальные сведения из теории групп. Аппарат теории групп является основным при изучении явлений симметрии, лежащих в основе фундаментальных закономерностей современного естествознания. Именно поэтому теория групп нашла широкое применение не только в современной математике, но и в ядерной физике, кристаллографии, теории относительности, различных разделах химии. Имеются опыты применения теоретико-групповых методов анализа в теории музыки, литературоведении, теории живописи, архитектуре. Математическая глубина и необычайно широкая сфера применений теории групп сочетаются с простотой ее основных положений, вполне доступных при наличии хорошо иллюстрирующих примеров школьникам старших классов. Поэтому теория групп как нельзя лучше подходит для того, чтобы показать школьникам образец современной математической теории и проиллюстрировать на примерах, как абстрактные теоретико-групповые понятия применяются при решении конкретных задач из разделов математики, уже знакомых читателю. Изучение понятия группы будет в достаточной степени оправдано, только если его применения будут разнообразны и интересны. Это одна из причин того, что основные теоретико-групповые понятия и результаты в книге излагаются в рамках теории групп перестановок конечных множеств. При таком изложении читатель постоянно работает с отображениями конечных множеств, что позволяет лучше усвоить понятия множества и функции — центральные понятия в школьном курсе математики.

При написании книги использовался опыт изложения основ теории групп на кружках и факультативных занятиях в республиканской физико-математической школе-интернате при Киевском государственном университете.

Первое издание книги, вышедшее в 1979 г.,— это выполненный Г. И. Фалиным перевод с украинского, который был дополнен авторами включением новых параграфов, касающихся приложений групп перестановок.

В настоящем издании по сравнению с первым расширены следующие параграфы: «Образующие симметрической группы», «Подгруппы симметрических групп. Группы перестановок», «Группы симметрий», «О решении алгебраических уравнений». Добавлены новые параграфы: «Теорема Кэли», «Перестановочные конструкции», «Венгерский шарнирный кубик», «Другие игры». Расширены и частично изменены подборки задач.

Киев

Л. А. Калужнин
В. И. Сущанский

§ 1. СУПЕРПОЗИЦИЯ ФУНКЦИЙ

Действие (или, иначе, операция) суперпозиции функций имеет ряд интересных свойств и много важных применений. Напомним определение и простейшие свойства суперпозиции для функций действительной переменной (функций, области определения и множества значений которых являются подмножествами множества действительных чисел).

Пусть $f(x)$ и $g(x)$ — произвольные функции действительной переменной. *Суперпозицией* этих функций (именно в том порядке, в котором они записаны) называется такая функция $h(x)$, что:

а) область определения $h(x)$ образована теми числами x_0 из области определения функции $f(x)$, для которых $f(x_0)$ принадлежит области определения функции $g(x)$;

б) значение функции $h(x)$ в какой угодно точке x_0 из области ее определения связано со значениями $f(x)$ и $g(x)$ равенством

$$h(x_0) = g(f(x_0)).$$

Таким образом, чтобы найти значение функции $h(x)$ в точке x_0, нужно найти $f(x_0) = y_0$, а затем $g(y_0)$. Число $g(y_0)$ и есть значение функции $h(x)$ в точке x_0.

Если функция $u(x)$ в точке x_0 принимает значение u_0, то это будем изображать так:

$$x_0 \xrightarrow{u} u(x_0) = u_0.$$

Читается такая схема одним из следующих способов: «функция $u(x)$ в точке x_0 принимает значение u_0», «функция $u(x)$ точке x_0 ставит в соответствие точку u_0», «точка u_0 является образом точки x_0 под действием функции $u(x)$». Для суперпозиции $h(x)$ функций $y = f(x)$ и $z = g(x)$ такая схема будет иметь вид

$$\underbrace{x_0 \xrightarrow{f} y_0 \xrightarrow{g} z_0}_{h}$$

(если функция $f(x)$ точке x_0 ставит в соответствие точку y_0, а функция $g(x)$ точке y_0 — точку z_0, то функция $h(x)$ точке x_0 ставит в соответствие точку z_0).

◀ Пример. Пусть $f(x)=x^2$, $g(x)=\sin x$. Чтобы найти значение суперпозиции $h(x)$ этих функций в некоторой точке x_0, нужно возвести x_0 в квадрат,

$$x_0 \xrightarrow{f} y_0 = x_0^2,$$

и найти значение $g(x)$ в точке y_0:

$$y_0 \xrightarrow{g} \sin y_0 = \sin(x_0^2).$$

Объединяя эти две схемы, получаем

$$\underbrace{x_0 \xrightarrow{f} y_0 = x_0^2 \xrightarrow{g} \sin(x_0^2)}_{h}.$$

Таким образом, функция $h(x)$ каждой точке x_0 ставит в соответствие $\sin(x_0^2)$, т. е. $h(x)$ можно задать формулой

$$h(x)=\sin(x^2).$$

Рассмотрим теперь суперпозицию $h_1(x)$ функций $g(x)=\sin x$ и $f(x)=x^2$, т. е. суперпозицию тех же самых функций, но в обратном порядке. Получим

$$\underbrace{x_0 \xrightarrow{\sin} \sin x_0 \xrightarrow{(\dots)^2} (\sin x_0)^2}_{h_1}.$$

Это означает, что суперпозиция функций $g(x)=\sin x$ и $f(x)=x^2$ есть функция

$$h_1(x)=(\sin x)^2=\sin^2 x. \ ▶$$

Таким образом, *суперпозиция функций зависит от порядка, в котором записаны функции.*

Будем обозначать суперпозицию функций $y=f(x)$ и $z=g(x)$ так: $(f\circ g)(x)$, т. е.

$$\underbrace{x \xrightarrow{f} y = f(x) \xrightarrow{g} z = g(y)}_{f\circ g}.$$

Следовательно,

$$(f\circ g)(x)=g(f(x)).$$

Особую роль относительно операции суперпозиции играет функция $y=x$, которую будем обозначать $e(x)$. Схема этой функции такая:

$$x_0 \xrightarrow{e} x_0$$

для каждого числа x_0. Очевидно, для любой функции $y=f(x)$ выполняются равенства

$$(f\circ e)(x)=(e\circ f)(x)=f(x),$$

или, в виде схемы,

$$\underbrace{x_0 \xrightarrow{f} y_0=f(x_0)\xrightarrow{e} y_0}_{f\circ e}, \quad \underbrace{x_0 \xrightarrow{e} x_0 \xrightarrow{f} y_0=f(x_0)}_{e\circ f}.$$

Дадим отдельное обозначение и для функции $y=-x$, а именно $e'(x)$.

Мы будем рассматривать множества функций, имеющих следующее свойство:

Если функции $f(x)$ и $g(x)$ принадлежат заданному множеству функций, то и суперпозиция $(f\circ g)(x)$ этих функций также принадлежит этому множеству.

О таком множестве говорят, что оно *замкнуто относительно операции суперпозиции функций*, или, иначе, что *суперпозиция является внутренней операцией* для такого множества.

Найдем, например, суперпозицию двух линейных функций. Пусть $f(x)=2x+5$, $g(x)=3x+1$. Для произвольного числа x_0 имеем

$$x_0 \xrightarrow{f} 2x_0+5=y_0 \xrightarrow{g} 3y_0+1=3(2x_0+5)+1,$$

т. е.

$$x_0 \xrightarrow{f\circ g} 3(2x_0+5)+1=6x_0+16,$$

а следовательно, $(f\circ g)(x)=6x+16$. Отсюда *суперпозиция двух заданных линейных функций снова есть линейная функция.*

Легко доказать, что это верно и в общем случае: если $f(x)=ax+b$, a $g(x)=cx+d$, то $(f\circ g)(x)=c(ax+b)+d=$ $=acx+bc+d=a_1x+b_1$, т. е. снова функция линейная. При этом коэффициенты этой функции выражаются через коэффициенты $f(x)$ и $g(x)$ с помощью равенств

$$a_1=ac, \quad b_1=bc+d.$$

Следовательно, множество всех линейных функций вместе с каждыми двумя функциями содержит и их суперпозицию, т. е. *суперпозиция является внутренней операцией для множества всех линейных функций*.

Результат суперпозиции для линейных функций также зависит, вообще говоря, от порядка их записи. Например, если $f(x)=2x+3$, а $g(x)=3x+2$, то $(f\circ g)(x)$ есть функция a_1x+b_1, причем $a_1=2\cdot 3=6$, $b_1=3\cdot 3+2=11$,

а $(g \circ f)(x)$ — это функция a_2x+b_2, где $a_2=3\cdot 2=6$, $b_2=2\cdot 2+3=7$. Следовательно, $(f\circ g)(x)=6x+11$, а $(g\circ f)(x)=6x+7$, т. е. для данных функций $(f\circ g)(x)\neq(g\circ f)(x)$.

Другим примером множества функций, замкнутого относительно суперпозиции, является множество всех многочленов вида

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

с целыми коэффициентами. Действительно, пусть

$$f(x)=c_0x^k+c_1x^{k-1}+\ldots+c_{k-1}x+c_k,$$
$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m$$

— два таких многочлена. Тогда суперпозицией $(f\circ g)(x)$, как легко убедиться, является такое выражение:

$$b_0(c_0x^k+c_1x^{k-1}+\ldots+c_k)^m+$$
$$+b_1(c_0x^k+c_1x^{k-1}+\ldots+c_k)^{m-1}+\ldots+b_m.$$

Это есть многочлен степени mk, который имеет вид

$$d_0x^{mk}+d_1x^{mk-1}+\ldots+d_{mk-1}x+d_{mk},$$

где коэффициенты d_0, d_1, ..., d_{mk} выражаются определенным образом через коэффициенты $f(x)$ и $g(x)$.

Общее правило для нахождения чисел d_0, d_1, ..., d_{mk} по известным коэффициентам c_0, ..., c_k, b_0, ..., b_m довольно громоздкое, но в каждом конкретном случае коэффициенты d_i удается вычислить без особых трудностей. Например, пусть

$$f(x)=x^2+2x+2,\quad g(x)=2x^2+x+2.$$

Тогда

$$(f\circ g)(x)=2(x^2+2x+2)^2+(x^2+2x+2)+2=$$
$$=2x^4+8x^3+17x^2+18x+12,$$
$$(g\circ f)(x)=(2x^2+x+2)^2+2(2x^2+x+2)+2=$$
$$=4x^4+4x^3+13x^2+6x+10\neq(f\circ g)(x).$$

В рассмотренных примерах множества функций, замкнутые относительно суперпозиции, были бесконечны. Однако это условие не является необходимым для замкнутости. Для множества, которое состоит лишь из двух функций $y=x$ и $y=-x$, которые мы обозначили $e(x)$ и $e'(x)$, суперпозиция также будет внутренней операцией.

Действительно,

$$(e \circ e)(x) = e(x),$$
$$(e \circ e')(x) = (e' \circ e)(x) = e'(x),$$
$$(e' \circ e')(x) = e(x),$$

т. е. условие замкнутости выполняется.

Даже из приведенных примеров видно, что множества, для которых суперпозиция является внутренней операцией, могут быть очень разными. Далее мы рассмотрим строение таких множеств для функций, определенных на конечных множествах.

Упражнения

1. Найти суперпозиции $(f \circ g)(x)$ и $(g \circ f)(x)$, где $y = f(x)$ и $y = g(x)$ — соответственно функции:

а) $y = 2x + 3$, $\quad y = 3x + 4$;

б) $y = x^3 + 5x^2$, $\quad y = x^2 + 3$;

в) $y = x^2 + 2$, $\quad y = x^3 + x + 1$;

г) $y = \frac{2x+3}{3x+2}$, $\quad y = \frac{x+4}{x-1}$.

2. Будут ли замкнуты относительно суперпозиции такие множества функций:

а) множество всех функций вида $y = ax$, где a — произвольное действительное число;

б) множество всех функций вида $y = x + a$, где a — произвольное рациональное число;

в) множество функций $y = x$, $y = 1/x$, $y = -1/x$, $y = -x$, каждая из которых рассматривается на множестве всех действительных чисел без нуля;

г) множество многочленов степени не выше 3-й;

д) множество функций $y = \frac{1}{1-x}$, $y = \frac{x-1}{x}$, $y = 1 - x$, $y = \frac{1}{x}$, $y = \frac{x}{x-1}$, $y = x$?

§ 2. ПРЕОБРАЗОВАНИЯ

Как известно, *отображением множества A в множество B* называется соответствие, по которому каждому элементу множества A сопоставляется однозначно определенный элемент множества B; этот элемент b называется *образом* элемента a; элемент a, в свою очередь, называется *прообразом* элемента b.

Отображения одного множества в другое будем обозначать строчными буквами греческого алфавита. Если задано отображение φ множества A в множество B, то

это обозначается одним из двух способов:

$$\varphi: A \to B, \qquad A \xrightarrow{\varphi} B.$$

Образ элемента $a \in A$ при отображении φ будем обозначать так: $(a)\varphi$ (знак отображения будем записывать справа от символа элемента).

Отображение одного множества в другое можно задавать описательно, указывая правило, по которому каждому элементу какого-то множества A ставится в соответствие его образ из множества B, а также с помощью таблиц, графиков, стрелочных схем.

Остановимся на указанных способах задания отображений произвольных множеств (как числовых, так и нечисловых). Строя таблицу отображения $\varphi: A \to B$, в нее записывают все возможные пары вида $(a, (a)\varphi)$, $a \in A$:

x	a_1	a_2	...	a_n
$(x)\varphi$	$(a_1)\varphi$	$(a_2)\varphi$	...	$(a_n)\varphi$

Такая таблица полностью задает отображение лишь тогда, когда множество A конечно и исчерпывается элементами $a_1, a_2, \ldots, a_n$.

Построение графиков отображений нечисловых множеств A, B несколько отличается от построения графиков числовых функций, с которым читатель хорошо знаком. Оно осуществляется так. Проводят два взаимно перпендикулярных луча, которые выходят из одной точки, — «оси координат». На горизонтальном луче произвольным способом (например, через одинаковые промежутки) отмечают точки, которые отвечают элементам множества A, а на вертикальном — точки, которые отвечают элементам множества B. Через эти точки проводят соответственно вертикальные и горизонтальные прямые, которые образуют прямоугольную сетку. Чтобы построить график отображения $\varphi: A \to B$, нужно поставить точки в тех вершинах сетки, «координатами» которых являются всевозможные пары вида $(a, (a)\varphi)$, где a — произвольный элемент множества A.

◀ Пример 1. Пусть $A = \{г, а, и, л\}$, $B = \{1, 2, 3, 4, 5, 6, 7\}$, а $\varphi: A \to B$ есть отображение, по которому каждой букве из множества A ставится в соответствие ее порядковый номер в слове «логарифм». График этого отображения дан на рис. 1. ▶

С помощью стрелочных схем, или, как их еще называют, *графов*, отображения множеств задают так: элементы множеств A и B обозначают различными точками плоскости (для множества A — слева, а для множества B — справа) и каждую из точек, которыми обозначены элементы множества A, соединяют стрелкой слева направо с точкой, которой обозначен соответствующий элемент множества B.

◀ Пример 2. Пусть $A=\{3, 2, 6, 7\}$, $B=\{28, 12, 4, 5, 11\}$, $\varphi: A \to B$ — отображение, которое каждому числу из A ставит в соответствие наименьшее общее кратное этого числа и числа 4. Это отображение полностью описывается стрелочной схемой, изображенной на рис. 2. Следовательно, имеем $(3)\varphi = 12$, $(2)\varphi = 4$, $(6)\varphi = 12$, $(7)\varphi = 28$. ▶

Рис. 1

Условимся обозначать число элементов конечного множества A символом $|A|$. Например, $|\{a, b, c, f\}| = 4$, $|\{1, 7, 10\}| = 3$ и т. п. Пусть множества A и B конечные и $|A| = m$, $|B| = n$. Ясно, что существует лишь конечное число различных отображений A в B, если считать разными отображения, которые действуют по-разному по меньшей мере на один элемент множества A.

Пользуясь тем, что каждое отображение A в B полностью описывается своей таблицей значений, подсчитаем, сколько именно существует разных отображений множества A в множество B.

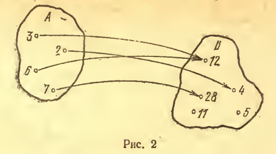


Рис. 2

Обозначим элементы множества A символами $a_1, a_2, \ldots, a_m$. Тогда таблицу каждого отображения A в B можно

будет записать так:

x	a_1	a_2	...	a_m
$x(\varphi)$	b_1	b_2	...	b_m

где $b_1, b_2, \ldots, b_m$ — обозначения некоторых, не обязательно разных элементов множества B. Верхний ряд таблицы одинаков для всех отображений A в B, а нижний меняется, потому что разным отображениям отвечают разные таблицы. При этом разных отображений A в B будет столько, сколькими разными способами можно заполнить второй ряд рассмотренной таблицы. В каждую клетку второго ряда таблицы можно записать обозначения любого элемента множества B. Таким образом, каждую из m клеток нижнего ряда таблицы отображения можно заполнить n разными способами независимо от способа заполнения других клеток. А это означает, что в таблице отображения можно образовать всего

$$\underbrace{n \cdot n \cdot \ldots \cdot n}_{m} = n^m$$

разных нижних рядов. Следовательно, существует n^m разных отображений A в B.

Выделяется и отдельно изучается несколько важных классов отображений одного множества в другое.

1. Отображение на все множество. Отображение $\varphi: A \to B$ называется *отображением на все множество* B или *сюръекцией*, если для каждого элемента $b \in B$ найдется такой элемент $a \in A$, что $(a)\varphi = b$.

◀ Примеры. 3. Пусть $A = \mathrm{R}$, $B = \mathrm{R}^+$ есть соответственно множество всех действительных и множество всех положительных действительных чисел. Зададим отображение $\varphi: \mathrm{R} \to \mathrm{R}^+$, положив $(x)\varphi = x^2$ для каждого $x \in \mathrm{R}$. Отображение φ будет сюръекцией, потому что для каждого числа $y \in \mathrm{R}^+$ существует по меньшей мере одно число $x \in \mathrm{R}$, такое, что $(x)\varphi = y$. Достаточно положить $x = \sqrt{y}$. Даже больше, для каждого $y \in \mathrm{R}^+$ существует точно два прообраза: $\sqrt{y}$, $-\sqrt{y}$.

4. Пусть $A = T$ — множество всех прямоугольных треугольников на плоскости, $B = \mathrm{R}^+$. Определим отображение $\varphi: T \to \mathrm{R}^+$ так: поставим в соответствие каждому прямоугольному треугольнику из T число, которое является его площадью при фиксированной единице измерения; φ есть сюръекция, так как для произвольного

$x \in R^+$ существует прямоугольный треугольник (с катетами $\sqrt{x}$ и $2\sqrt{x}$), который имеет площадь x. Существует даже бесконечно много прямоугольных треугольников, которые имеют площадь x (например, треугольники с катетами $\sqrt{x}/k$, $2k\sqrt{x}$, $k = 1, 2, 3, \ldots$). Следовательно, тут каждый элемент $x \in R^+$ имеет бесконечно много прообразов.

5. Пусть S — множество трехзначных простых чисел, а L — множество цифр. Отображение $\varphi: S \to L$ определим так: поставим в соответствие каждому трехзначному простому числу его вторую цифру. Например:

$$(179)\varphi = 7, \qquad (821)\varphi = 2, \qquad (907)\varphi = 0.$$

Непосредственной проверкой убеждаемся, что φ — сюръекция, т. е. для каждой цифры найдется трехзначное простое число, в котором эта цифра стоит посередине. Тут множества S и L конечны, и для каждого элемента из L существует лишь конечное число элементов из S, которые на него отображаются. ▶

Если множества A и B конечны и $\varphi: A \to B$ — сюръекция, то в нижнем ряду ее таблицы встречаются все элементы из B. На каждой горизонтальной прямой графика сюръекции обязательно есть обозначенные вершины сетки. На стрелочной схеме сюръекции в каждую точку, которая обозначает элемент множества B, входит по меньшей мере одна стрелка.

Сюръекция конечного множества A на множество B существует не всегда. Очевидно, для этого необходимо, чтобы множество B также было конечно и выполнялось неравенство $|A| \geq |B|$.

2. Взаимно однозначное отображение. *Отображение* $\varphi: A \to B$ *называется взаимно однозначным* или *инъекцией*, если разные элементы множества A переводятся этим отображением в разные элементы множества B: для каждых $x_1, x_2 \in A$ из $x_1 \neq x_2$ вытекает $(x_1)\varphi \neq (x_2)\varphi$.

◀ Примеры. 6. Отображение φ множества целых чисел $\mathbf{Z}$ в множество всех четных чисел $2\mathbf{Z}$ определим так: положим $z(\varphi) = 6z$ для каждого $z \in \mathbf{Z}$. Это отображение — инъекция, так как из $z_1 \neq z_2$ вытекает $6z_1 \neq 6z_2$.

7. Пусть A — множество всевозможных двухэлементных подмножеств множества действительных чисел $\mathbf{R}$, B — множество приведенных квадратных уравнений. Каждому элементу $\{a, b\}$ множества A поставим в соответствие уравнение из B, для которого числа a, b являются кор-

нями. Как вытекает из теоремы Виета, такое отображение будет инъективным. ▶

В нижнем ряду таблицы инъективного отображения $\varphi: A \to B$ в отличие от таблиц произвольных отображений, каждый элемент множества B встречается лишь один раз. Следовательно, на каждой горизонтальной прямой графика инъекции обозначено не более одной вершины сетки, а при стрелочном изображении инъекции в каждую точку, которой обозначается элемент множества B, входит не более чем одна стрелка.

Если множества A и B конечны и существует инъекция множества A в множество B, то, очевидно, должно выполняться неравенство

$$|A| \leqslant |B|.$$

3. Взаимно однозначное отображение на все множество. Если отображение φ множества A в множество B является одновременно инъективным и сюръективным, то оно называется *взаимно однозначным отображением множества A на множество B* или *биекцией A на B*.

◀ Примеры. 8. Пусть $A = B = \Pi$ — множество точек плоскости. Тогда биекцией является каждое из следующих известных из школьного курса геометрии отображений множества Π на себя: симметрия относительно фиксированной точки, симметрия относительно фиксированной прямой, параллельный перенос, поворот вокруг фиксированной точки, гомотетия.

9. Отображение $\varphi: x \to 2x$, где $x \in \mathbf{Z}$, есть, очевидно, биекция множества $\mathbf{Z}$ на множество $2\mathbf{Z}$ четных чисел. ▶

Если существует биекция конечного множества A на конечное множество B, то должны выполняться неравенства $|A| \geqslant |B|$ и $|A| \leqslant |B|$. Следовательно, для конечных множеств A и B биекция A на B существует тогда и только тогда, когда выполняется равенство $|A| = |B|$.

Подсчитаем, сколько существует разных биекций множества $A = \{a_1, a_2, \ldots, a_n\}$ на множество $B = \{b_1, b_2, \ldots, b_n\}$.

Каждая биекция $\varphi: A \to B$ полностью описывается своей таблицей:

x	a_1	a_2	...	a_n
$x(\varphi)$	b_1	b_2	...	b_n

Верхний ряд таблицы не меняется, а в нижнем ряду могут стоять произвольно размещенные обозначения эле-

ментов множества B, причем обязательно разных. Следовательно, первое (например, слева) место нижнего ряда таблицы можно заполнить n разными способами. Если первое место уже заполнено, то независимо от того, каким элементом оно заполнено, на второе место можно поставить обозначение какого угодно из тех элементов множества B, которые остались. Аналогично третью клетку, независимо от того, какие элементы поставлены в первые две клетки, можно заполнить $n-2$ способами и т. д. Для предпоследнего места остаются лишь две возможности его заполнения, а для последнего — только одна. Поскольку каждая клетка заполняется независимо от остальных, существует

$$n(n-1)(n-2)\ldots 2\cdot 1=n!$$

разных способов одновременного заполнения клеток. Следовательно, можно составить $n!$ разных таких таблиц, т. е. существует $n!$ разных биекций A на B.

Очень часто приходится рассматривать отображения некоторого множества M в себя. Такие отображения называются еще *преобразованиями* множества M. Читателю хорошо известны, например, разные типы геометрических преобразований, которые уже упоминались в примере 8.

Для преобразований произвольного множества также можно рассмотреть введенные выше классы отображений: инъекции, биекции и сюръекции. Но для конечных множеств, как легко понять, эти три класса преобразований совпадают, т. е. *каждая инъекция конечного множества в себя будет также и сюръекцией, а каждая сюръекция есть одновременно и инъекция.* А поэтому для конечных множеств выделяется лишь класс биективных преобразований.

Изучая преобразования произвольного конечного множества, удобно придерживаться определенных стандартных обозначений. Природа элементов множества M при изучении его преобразований несущественна. Следовательно, мы можем занумеровать все элементы множества M и оперировать не с самими элементами, а с их номерами. Поэтому, рассматривая преобразования конечных множеств, мы будем впредь иметь в виду множество

$$M=\{1,\ 2,\ 3,\ \ldots,\ n\}$$

первых n натуральных чисел.

Задавая преобразования таблицами, будем записывать их в таком упрощенном виде:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}.$$

Ясно, что такое обозначение однозначно характеризует преобразование и не вызывает недоразумений. Например, если $M = \{1, 2, 3, 4, 5\}$, то

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 2 & 5 \end{pmatrix}$, б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

есть таблицы разных преобразований на множестве M. Читать такую таблицу, например а), следует так:

«Преобразование φ, заданное таблицей а),

1 переводит в 2,
2 переводит в 2,
3 переводит в 4,
4 переводит в 2,
5 переводит в 5».

Порядок записи элементов верхнего ряда такой таблицы не существен. Например, преобразование, заданное таблицей б), можно обозначить также таблицами:

$$\begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \begin{pmatrix} 5 & 4 & 1 & 2 & 3 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

Поскольку каждое преобразование конечного множества полностью описывается своей таблицей, мы часто будем обозначать одинаковыми символами само преобразование и его таблицу.

Некоторые преобразования множества M имеют специальные названия.

а) Тождественное преобразование. *Тождественное преобразование* — это преобразование ε, которое все элементы из M оставляет на месте, т. е. $(a)\varepsilon = a$ для каждого $a \in M$. Если M — конечное множество, это преобразование будет иметь таблицу

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & 2 & 3 & \dots & n-1 & n \end{pmatrix}.$$

б) Постоянное преобразование. Преобразование называется *постоянным*, если оно каждому элементу из M ставит в соответствие некоторый фиксированный элемент этого множества. Если M — конечное множество,

постоянное преобразование характеризуется таблицей вида

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ a & a & a & \dots & a & a \end{pmatrix},$$

где $a \in M$.

в) Перестановки. *Перестановкой* будем называть биекцию конечного множества на себя. Следовательно, φ есть перестановка на M тогда и только тогда, когда для произвольных элементов $a, b \in M$, $a \neq b$, имеем $(a)\varphi \neq (b)\varphi$. А это означает, что перестановка определяется таблицей вида

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \end{pmatrix},$$

где $a_1, a_2, \dots, a_n$ — разные элементы из M.

Упражнения

1. Построить графики и стрелочные схемы для отображений множества $\{1, 2, 3, 4, 5\}$ в множество $\{a, b, c, d\}$, заданных такими таблицами:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & b & a \end{pmatrix}$, б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & a & a & c & a \end{pmatrix}$, в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & a & b & c \end{pmatrix}$.

2. Пусть A и B — конечные множества, причем $|A| = m$, $|B| = n$. Сколько существует разных инъекций множества A в множество B?

3. Пользуясь решением предыдущего упражнения, найти, сколько существует m-элементных подмножеств множества из n элементов.

4. Будет ли сюръекцией отображение $\varphi: S \to L$ из множества S слов русского языка в множество L букв русского алфавита, которое каждому слову ставит в соответствие его первую букву?

5. Какие свойства отличают графики и стрелочные схемы биекций от графиков и стрелочных схем произвольных отображений?

6. Сколькими способами можно расположить n одноцветных ладей на шахматной доске с n^2 клетками так, чтобы никакие две из них не били друг друга?

7. Сколько существует разных перестановок на множестве $M = \{1, 2, 3, 4, 5\}$, которые ни один элемент из M не оставляют на месте (т. е. для таких перестановок φ имеем $a(\varphi) \neq a$ для каждого $a \in M$)?

8. Сколькими способами можно расположить на шахматной доске 8 одноцветных ладей так, чтобы никакая из них не стояла на белой диагонали и никакие две не били друг друга?

9. Сколько можно составить разных шестизначных чисел из цифр 0, 1, 2, 3, 4, 7, 9?

10. Сколько существует разных перестановок φ на множестве $\{1, 2, 3, \dots, n\}$, для которых $(1)\varphi - (2)\varphi > 1$?

11. Доказать, что при $n \geq 4$ существует перестановка φ множества $M = \{1, 2, \dots, n\}$, для которой при любых $i, j \in M$ выполняется условие $|(i)\varphi - j(\varphi)| = |i - j|$.

12. Доказать, что при $n \geq 4$ существует размещение n одноцветных ферзей на шахматной доске с n^2 клетками, при котором никакие 2 ферзя не бьют друг друга.

13. Сколькими способами можно разместить 8 одноцветных ферзей на шахматной доске так, чтобы никакие 2 из них не били друг друга?

§ 3. УМНОЖЕНИЕ ПРЕОБРАЗОВАНИЙ

В § 1 мы рассмотрели операцию образования суперпозиции функций, заданных на множестве действительных чисел. Аналогично можно строить новое преобразование по двум данным и для произвольных множеств.

Пусть M — произвольное множество, φ и ψ — некоторые преобразования этого множества. *Произведением преобразований* φ, ψ называется такое преобразование ω множества M, которое на каждый элемент $a \in M$ действует так:

$$(a)\,\omega = ((a)\varphi)\psi, \tag{1}$$

т. е., чтобы найти образ произвольного элемента $a \in M$ под действием преобразования ω, нужно сначала найти образ b элемента a под действием преобразования φ, а потом — образ c элемента b под действием преобразования ψ. Элемент c и есть образ элемента a под действием преобразования ω.

Рис. 3

На языке стрелочных схем действие преобразования ω на элемент $a \in M$ можно выразить так:

$$a \xrightarrow{\varphi} b \xrightarrow{\psi} c, \quad a \xrightarrow{\omega} c$$

Произведение преобразований φ, ψ будем обозначать далее через $\varphi \circ \psi$.

◀ Примеры. 1. Пусть M — множество людей, которые когда-либо жили на Земле, φ — преобразование множества M, которое каждому человеку ставит в соответствие его отца, а ψ — преобразование множества M, которое каждому человеку ставит в соответствие его мать. Тогда:

а) $\varphi \circ \psi$ — преобразование множества M, которое каждому человеку ставит в соответствие бабушку по отцовской линии;

б) $\varphi \circ \varphi$ — преобразование множества M, которое каждому человеку ставит в соответствие дедушку по отцовской линии;

в) $\psi\circ\varphi$ — преобразование множества M, которое каждому человеку ставит в соответствие его дедушку по материнской линии;

г) $\psi\circ\psi$ — преобразование множества M, которое каждому человеку ставит в соответствие его бабушку по материнской линии.

2. Пусть $M=\Pi$ — множество точек плоскости, φ — поворот плоскости вокруг фиксированной точки O на угол $\pi/2$ по часовой стрелке, а ψ — поворот плоскости вокруг точки на угол $2\pi/3$ против часовой стрелки. Тогда и $\varphi\circ\psi$ и $\psi\circ\varphi$ — поворот на угол $\pi/6$ против часовой стрелки (рис. 3).

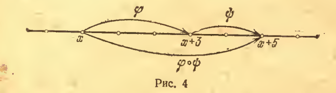


Рис. 4

3. Пусть $\varphi: x\to x+3$ — преобразование множества действительных чисел $\mathbf{R}$, которое числу x ставит в соответствие число $x+3$, а $\psi: x\to x+2$ — преобразование этого множества, которое каждое число x переводит в число $x+2$. Тогда $\varphi\circ\psi=\psi\circ\varphi$ — преобразование, которое каждое число x переводит в число $x+5$ (рис. 4). ▶

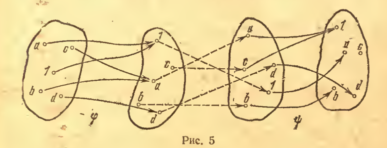


Рис. 5

Очень легко найти произведение двух преобразований, заданных стрелочными схемами. Поясним это на примере. Пусть φ и ψ — преобразования множества $M=\{a, b, c, d, 1\}$, стрелочные схемы которых изображены на рис. 5. Чтобы построить стрелочную схему преобразования $\varphi\circ\psi$, нужно соединить стрелками те точки правой части стрелочной схемы φ и левой части стрелочной схемы ψ, которые обозначают одинаковые элементы из M (на рис. 5 эти

стрелки изображены штриховыми линиями). Получаем единую схему, по которой образ произвольного элемента из M при преобразовании $\varphi\circ\psi$ находим так: из каждой точки левой части стрелочной схемы преобразования φ проходим вдоль стрелок до соответствующей точки правой части стрелочной схемы преобразования ψ. Получим

$$(a)(\varphi\circ\psi)=a,\quad (b)(\varphi\circ\psi)=1,\quad (c)(\varphi\circ\psi)=1,$$
$$(d)(\varphi\circ\psi)=d,\quad (1)(\varphi\circ\psi)=a.$$

Следовательно, преобразование $\varphi\circ\psi$ имеет стрелочную схему, изображенную на рис. 6.

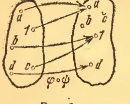


Рис. 6

Т а б л и ц у   п р о и з в е д е н и я   п е р е с т а н о в о к

$$\varphi=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ i_1 & i_2 & i_3 & \dots & i_n\end{pmatrix},$$
$$\psi=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ j_1 & j_2 & j_3 & \dots & j_n\end{pmatrix}$$

находят по такому удобному правилу:

а) переставляют столбцы в таблице ψ так, чтобы ее верхний ряд совпадал с нижним рядом таблицы φ, и получают

$$\psi'=\begin{pmatrix}i_1 & i_2 & i_3 & \dots & i_n\\ k_1 & k_2 & k_3 & \dots & k_n\end{pmatrix};$$

б) строят новую таблицу, первым рядом которой является первый ряд таблицы φ, а вторым — второй ряд таблицы ψ'.

Построенная таблица и будет таблицей преобразования $\varphi\circ\psi$.

◀ П р и м е р 4. Пусть

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 4 & 1 & 6 & 2 & 5\end{pmatrix},\quad \psi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 2 & 1\end{pmatrix}.$$

Имеем

$$\varphi\circ\psi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 4 & 1 & 6 & 2 & 5\end{pmatrix}\circ\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 2 & 1\end{pmatrix}=$$
$$=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 4 & 1 & 6 & 2 & 5\end{pmatrix}\circ\begin{pmatrix}3 & 4 & 1 & 6 & 2 & 5\\ 4 & 3 & 6 & 1 & 5 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 3 & 6 & 1 & 5 & 2\end{pmatrix}. ▶$$

В предыдущем параграфе были рассмотрены три класса преобразований произвольного множества: инъекции, сюръекции и биекции. Оказывается, что *каждый из этих классов замкнут относительно умножения преобразований*,

т. е. произведение инъекций снова инъекция, произведение сюръекций — сюръекция и, наконец, произведение биекций — биекция.

Действительно, пусть преобразования φ и ψ являются инъекциями множества M в себя и $\omega=\varphi\circ\psi$. Тогда для каждой пары элементов $a,\ b\in M,\ a\neq b$, будем иметь

$$(a)\varphi\neq(b)\varphi,\quad (a)\psi\neq(b)\psi.$$

Подействуем преобразованием ω на элементы a и b. По определению произведения преобразований

$$(a)\omega=((a)\varphi)\psi=(a_1)\psi,\quad (b)\omega=((b)\varphi)\psi=(b_1)\psi,$$

где $a_1=(a)\varphi$, $b_1=(b)\varphi$. Поскольку φ — инъекция, то $a_1\neq b_1$. В свою очередь, поскольку ψ — инъекция, имеем $(a_1)\psi\neq\neq(b_1)\psi$. Значит, для каждой пары $a,\ b\in M,\ a\neq b$, имеем $(a)\omega\neq(b)\omega$, и ω является инъекцией.

Пусть теперь преобразования φ и ψ сюръективны. Убедимся, что для каждого элемента $a\in M$ найдется такой элемент $b\in M$, для которого $(b)\omega=a$. Поскольку ψ — сюръекция, найдется такой элемент $c\in M$, что $(c)\psi=a$, а из сюръективности φ вытекает, что существует такой элемент $b\in M$, для которого $(b)\varphi=c$. Элемент b искомый:

$$(b)\omega=((b)\varphi)\psi=(c)\psi=a.$$

Следовательно, преобразование ω — сюръекция.

Отсюда сразу же получаем, что произведение биективных преобразований — преобразование биективное. В частности, *для конечных множеств все три класса преобразований совпадают*, т. е. *произведение произвольных двух перестановок на множестве M снова является перестановкой на множестве M*. Это следует также из описанного нами правила нахождения произведения перестановок.

Как известно, операции сложения и умножения чисел характеризуются рядом свойств. Например, операция сложения чисел имеет такие свойства (именно операция сложения, а не сами числа):

а) Ассоциативность. Для каждых трех чисел $a,\ b,\ c$ справедливо равенство

$$a+(b+c)=(a+b)+c.$$

б) Коммутативность. Для каждых двух чисел $a,\ b$ выполняется равенство

$$a+b=b+a.$$

в) Существует нейтральный элемент (нуль), такой, что для любого числа a

$$a+0=0+a=a.$$

г) Для каждого числа a существует противоположное к нему число $-a$, такое, что

$$a+(-a)=0.$$

Выясним, справедливы ли отмеченные свойства для операции умножения преобразований произвольного множества M.

а) Умножение преобразований произвольного множества M имеет свойство ассоциативности. Это означает, что для каждых трех преобразований α, β, γ множества M справедливо равенство

$$(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma). \tag{2}$$

Оно свидетельствует о том, что на любой элемент $a \in M$ преобразования $\varphi = (\alpha \circ \beta) \circ \gamma$ и $\psi = \alpha \circ (\beta \circ \gamma)$ действуют одинаково:

$$(a)\,((\alpha \circ \beta) \circ \gamma) = (a)\,(\alpha \circ (\beta \circ \gamma)). \tag{3}$$

Действительно, возьмем произвольный элемент $a \in M$, и пусть $(a)\alpha = b$, $(b)\beta = c$, $(c)\gamma = d$. Тогда по определению (1)

$$(a)\varphi = ((a)\,(\alpha \circ \beta))\gamma = (((a)\alpha)\beta)\gamma = ((b)\beta)\gamma = (c)\gamma = d,$$
$$(a)\psi = ((a)\alpha)\,(\beta \circ \gamma) = (b)\,(\beta \circ \gamma) = ((b)\beta)\gamma = (c)\gamma = d.$$

Таким образом, равенство (3) выполняется для произвольного $a \in M$, и, следовательно, справедливо равенство (2).

На рис. 7 изображено схематично действие произведения преобразований на элемент $a \in M$. Произведению $\alpha \circ (\beta \circ \gamma)$ отвечает путь, обозначенный линией из жирных точек, а произведению $(\alpha \circ \beta) \circ \gamma$ — путь, обозначенный штриховой линией. Обе линии заканчиваются в точке, которая отвечает элементу $d \in M$, т. е. преобразования φ и ψ действуют на элемент a одинаково. Следовательно, операция умножения преобразований множества M ассоциативна.

б) Умножение преобразований произвольного множества не коммутативно. Это означает, что существуют такие преобразования φ и ψ заданного множества M, для которых

$$\varphi \circ \psi \neq \psi \circ \varphi.$$

Такими преобразованиями на соответствующих множествах являются преобразования φ, ψ, приведенные в примерах 1 и 4.

Не следует думать, что произведение преобразований всегда зависит от порядка, в котором записаны сомножители. Например, произведение преобразований, определенных в примерах 2 и 3, не зависит от порядка сомножителей. Произведение перестановок

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 3 & 1 & 6 & 5 & 4\end{pmatrix} \quad \text{и} \quad \psi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 2 & 4 & 5 & 6\end{pmatrix}$$

также не зависит от порядка их записи:

$$\varphi\circ\psi=\psi\circ\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 2 & 3 & 6 & 5 & 4\end{pmatrix}.$$

в) Особую роль при умножении преобразований играют тождественное преобразование ε и постоянные преобразования δ_x, $x\in M$ (напомним, что $(a)\varepsilon=a$ и $(a)\delta_x=x$ для

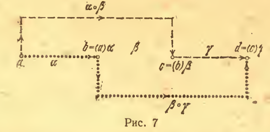


Рис. 7

каждого $a\in M$). Преобразование ε играет для операции умножения преобразований ту же роль, что и единица при умножении чисел (или нуль при сложении чисел), т. е. для каждого преобразования φ множества M имеем

$$\varphi\circ\varepsilon=\varepsilon\circ\varphi=\varphi. \tag{4}$$

Действительно, положив $(a)\varphi=b$, по определению произведения (1) для каждого элемента $a\in M$ будем иметь

$$(a)(\varphi\circ\varepsilon)=((a)\varphi)\varepsilon=(b)\varepsilon=b,$$
$$(a)(\varepsilon\circ\varphi)=((a)\varepsilon)\varphi=(a)\varphi=b.$$

Это и означает, что справедливо равенство (4).

Легко понять, что ε — *единственное преобразование, для которого выполняются равенства* (4). Действительно, допустим, что существует другое преобразование $\varepsilon'\neq\varepsilon$,

такое, что для каждого φ имеем

$$\varepsilon' \circ \varphi = \varphi \circ \varepsilon' = \varphi.$$

Тогда произведение $\varepsilon \circ \varepsilon' = \varepsilon' \circ \varepsilon$, с одной стороны, должно равняться ε' (когда роль единицы выполняет ε), а с другой — ε (когда роль единицы выполняет ε'). Следовательно,

$$\varepsilon = \varepsilon \circ \varepsilon' = \varepsilon',$$

а потому $\varepsilon = \varepsilon'$, и мы пришли к противоречию, которое свидетельствует о том, что наше допущение неверно.

Преобразования δ_x (их столько, сколько элементов имеет множество M) относительно умножения играют роль «нулей», т. е. для любого преобразования φ имеем

$$\varphi \circ \delta_x = \delta_x.$$

Но

$$\delta_x \circ \varphi = \delta_{(x)\varphi}$$

(проверьте!).

◀ Пример 5. Пусть

$$M = \{1,\ 2,\ 3,\ 4,\ 5\}, \qquad \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Тогда

$$\varphi \circ \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix},$$

$$\delta_2 \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 \end{pmatrix}$$

(тут $4 = (2)\varphi$).

Следовательно, если произвольное преобразование умножить на «нуль» справа, то получим тот же самый «нуль», а если слева, «нуль», вообще говоря, будет другой. ▶

г) *Обратным для преобразования α произвольного множества M называется такое преобразование β этого множества, что справедливы равенства*

$$\alpha \circ \beta = \beta \circ \alpha = \varepsilon.$$

Это преобразование выполняет ту же роль, что и противоположное число для операции сложения чисел или обратное число для операции умножения чисел. Так же как и обратное число a^{-1} (которое существует только для $a \neq 0$), *преобразование, обратное к данному, может существовать, а может и не существовать.* Например, обратным к преобразованию

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

является преобразование

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix},$$

а для постоянных преобразований обратных преобразований не существует. Но в тех случаях, *когда обратное преобразование существует, оно единственно.*

Действительно, допустим, что для некоторого преобразования φ множества M существует два обратных преобразования φ_1 и φ_2, $\varphi_1 \neq \varphi_2$, т. е. одновременно выполняются равенства

$$\varphi \circ \varphi_1 = \varphi_1 \circ \varphi = \varepsilon, \quad \varphi \circ \varphi_2 = \varphi_2 \circ \varphi = \varepsilon.$$

Из этих равенств и свойства ассоциативности действия умножения преобразований последовательно имеем

$$\varphi_1 = \varphi_1 \circ \varepsilon = \varphi_1 \circ (\varphi \circ \varphi_2) = (\varphi_1 \circ \varphi) \circ \varphi_2 = \varepsilon \circ \varphi_2 = \varphi_2,$$

и мы пришли к противоречию, которое свидетельствует о том, что наше допущение неверно.

Единственное преобразование, обратное к преобразованию φ, далее будем обозначать φ^{-1}.

Когда же существует обратное преобразование? Исчерпывающий ответ на этот вопрос дает такая теорема.

Теорема. *Преобразование, обратное к преобразованию α множества M, существует тогда и только тогда, когда α является биекцией множества M.*

Доказательство. Необходимость. Пусть для преобразования α существует обратное к нему преобразование β, т. е. $\alpha \circ \beta = \beta \circ \alpha = \varepsilon$. Тогда для каждого $y \in M$ имеем $y = (y)\,\varepsilon = (y)\,(\beta \circ \alpha) = ((y)\beta)\alpha = z\,(\alpha)$, где $z = (y)\beta$. Следовательно, для каждого $y \in M$ существует элемент $z \in M$, такой, что $(z)\alpha = y$, и α — сюръекция.

Покажем, что преобразование α будет также инъекцией. Допустим, что это не так. Тогда найдутся различные элементы $a, b \in M$, для которых $(a)\alpha = (b)\alpha = c$. Поэтому будем иметь

$$((a)\alpha)\beta = ((b)\alpha)\beta = (c)\beta,$$

или

$$(a)\,(\alpha \circ \beta) = (b)\,(\alpha \circ \beta) = (c)\beta,$$

откуда

$$(a)\varepsilon = (b)\varepsilon \quad \text{и} \quad a = b.$$

Мы пришли к противоречию, которое и доказывает, что α — инъекция.

Достаточность. Пусть α — биективное преобразование. Тогда для каждого $x \in M$ существует единственный прообраз — такой элемент $y \in M$, что $(y)\alpha = x$. Поэтому можно определить такое преобразование β множества M, которое ставит в соответствие каждому элементу $x \in M$ его прообраз y при преобразовании α:

$$\text{если} \quad y \xrightarrow{\alpha} x, \quad \text{то} \quad x \xrightarrow{\beta} y.$$

β действительно является преобразованием, так как, поскольку α — сюръекция, оно определено для каждого элемента из M. Из самого определения β вытекает, что выполняются равенства

$$((x)\alpha)\beta = x \quad \text{и} \quad ((x)\beta)\alpha = x$$

для каждого $x \in M$. Это означает, что $\alpha \circ \beta = \beta \circ \alpha = \varepsilon$, т. е. β — преобразование, обратное к α.

Теорема доказана.

Пользуясь этой теоремой, легко решить вопрос о существовании обратной функции. *Обратной для функции* $f(x)$ называется такая функция $g(x)$, что $(f \circ g)(x) = (g \circ f)(x) = x$.

Для того чтобы функция $f(x)$ имела обратную, необходимо и достаточно, чтобы она осуществляла биективное отображение области своего определения на множество своих значений.

Очевидно, *преобразования α и α^{-1} взаимно обратны, т. е. каждое из них обратно к другому. Следовательно,* $(\alpha^{-1})^{-1} = \alpha$.

◀ Примеры. 6. Пусть φ — поворот плоскости на угол $2\pi/3$ против часовой стрелки вокруг точки O. Поскольку φ — биекция, φ^{-1} существует. Легко понять, что φ^{-1} — поворот плоскости на угол $2\pi/3$ по часовой стрелке вокруг точки O.

7. Функции $y = 2x + 3$, $y = x^3$ — биективные преобразования

$$x \to 2x + 3, \qquad x \to x^3$$

множества действительных чисел $\mathbb{R}$ на себя. Поэтому для них существуют обратные преобразования, а именно

$$x \to \frac{x-3}{2}, \qquad x \to \sqrt[3]{x}.$$

Следовательно, функции $y = \frac{x-3}{2}$ и $y = \sqrt[3]{x}$ обратны соответственно к функциям $y = 2x + 3$, $y = x^3$.

Функции $y=x^2$, $y=\sin x$ — преобразования

$$x \to x^2, \qquad x \to \sin x$$

множества $\mathbf{R}$, которые не биективны. А поэтому для них не существует обратных. Однако можно рассмотреть ограничение функции $y=x^2$ на множество $\mathbf{R}^+ \cup \{0\}$ неотрицательных действительных чисел. Это функция, область определения которой есть множество $\mathbf{R}^+ \cup \{0\}$, причем во всех точках области определения она совпадает с функцией $y=x^2$. Это ограничение будет биективным преобразованием множества $\mathbf{R}^+ \cup \{0\}$, т. е. для него существует обратное преобразование $x \to \sqrt{x}$. Таким образом, функция $y=\sqrt{x}$ обратна к ограничению функции $y=x^2$ на множество $\mathbf{R}^2 \cup \{0\}$ (а не к функции $y=x^2$, как часто говорят).

Вполне аналогично можно рассмотреть ограничение функции $y=\sin x$ на промежуток $[-\pi/2, \pi/2]$. Это ограничение является биективным отображением множества $[-\pi/2, \pi/2]$ на множество $[-1, 1]$. Следовательно, для него существует обратное — функция $y=\arcsin x$.

8. Пусть преобразование φ множества точек плоскости является параллельным переносом в заданном направлении на расстояние d. Ясно, что φ — биективное преобразование, следовательно, для него существует обратное. Это также параллельный перенос на то же самое расстояние, но в противоположном направлении. ▶

Для преобразования конечного множества M существует обратное преобразование тогда и только тогда, когда оно является перестановкой. Пусть дана перестановка

$$\varphi=\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix};$$

тогда обратная к ней перестановка, как вытекает из правила умножения перестановок, будет такая:

$$\varphi^{-1}=\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Ее столбцы можно переставить так, чтобы числа верхнего ряда были расположены в порядке возрастания. Например, обратной к перестановке

$$\varphi=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 5 & 7 & 6 & 3 \end{pmatrix}$$

будет перестановка

$$\varphi^{-1}=\begin{pmatrix} 4 & 2 & 1 & 5 & 7 & 6 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 1 & 4 & 6 & 5 \end{pmatrix}.$$

Для преобразований произвольного множества можно составлять и решать уравнения. Как пример рассмотрим уравнения первой степени. Пусть φ, ψ — произвольные преобразования множества M. Существуют ли такие преобразования x у этого множества, для которых выполнялись бы равенства

$$\varphi \circ x = \psi, \tag{5}$$

$$y \circ \varphi = \psi\ ? \tag{6}$$

Если такие преобразования существуют, то единственны ли они? Подчеркнем, что следует рассматривать оба уравнения, так как операция умножения преобразований некоммутативна и эти уравнения могут иметь разные решения.

Довольно легко ответить на вопрос о существовании и единственности решения для уравнений (5) и (6), в которых «коэффициент» φ — перестановка.

Если φ — перестановка, то решения уравнений (5) *и* (6) *существуют и единственны.*

Доказывается этот факт следующим образом. Поскольку φ — биекция, для него существует обратное преобразование φ^{-1}. Можно поэтому рассмотреть преобразования $\varphi^{-1} \circ \psi$ и $\psi \circ \varphi^{-1}$ (отметим, что, вообще говоря, $\varphi^{-1} \circ \psi \neq \psi \circ \varphi^{-1}$, так как операция умножения преобразований некоммутативна). Покажем, что $\varphi^{-1} \circ \psi$ будет решением уравнения (5). Для этого вычислим произведение $\varphi \circ (\varphi^{-1} \circ \psi)$. Используя ассоциативность операции умножения преобразований и определение обратного преобразования, получим

$$\varphi \circ (\varphi^{-1} \circ \psi) = (\varphi \circ \varphi^{-1}) \circ \psi = \varepsilon \circ \psi = \psi.$$

А это и означает, что $\varphi^{-1} \circ \psi$ — решение уравнения (5). Аналогично доказывается, что преобразование $\psi \circ \varphi^{-1}$ — решение уравнения (6).

Теперь докажем, что указанные решения уравнений (5) и (6) единственны. Действительно, если преобразования α и β — решения уравнений (5) и (6) соответственно,

$$\varphi \circ \alpha = \psi, \tag{7}$$

$$\beta \circ \varphi = \psi, \tag{8}$$

то, умножая равенство (7) слева на φ^{-1}, а равенство (8) справа на φ^{-1}, получим

$$\varphi^{-1} \circ (\varphi \circ \alpha) = \varphi^{-1} \circ \psi, \quad (\beta \circ \varphi) \circ \varphi^{-1} = \psi \circ \varphi^{-1},$$

т. е.

$$(\varphi^{-1}\circ\varphi)\circ\alpha=\varphi^{-1}\circ\psi,\quad \beta\circ(\varphi\circ\varphi^{-1})=\psi\circ\varphi^{-1},$$

или

$$\varepsilon\circ\alpha=\varphi^{-1}\circ\psi,\quad \alpha=\varphi^{-1}\circ\psi,$$
$$\beta\circ\varepsilon=\psi\circ\varphi^{-1},\quad \beta=\psi\circ\varphi^{-1}.$$

Эти равенства означают, что никаких других решений, кроме отмеченных ранее, уравнения (5) и (6) не имеют.

◄ Пример 9. Пусть $M=\{1, 2, 3, 4\}$,

$$\varphi=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\quad \psi=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}.$$

Нетрудно проверить, что решением уравнения (5) будет перестановка

$$\varphi^{-1}\circ\psi=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},$$

а решением уравнения (6) — перестановка

$$\psi\circ\varphi^{-1}=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}\neq\varphi^{-1}\circ\psi.\ ►$$

Если преобразование φ в уравнениях (5) и (6) — не перестановка, то эти уравнения могут иметь решения, а могут и не иметь их (см. упражнения 8 — 11).

Упражнения

1. Доказать, что произведение параллельных переносов снова будет параллельным переносом.

2. Изобразить преобразования, заданные таблицами, с помощью стрелочных схем и найти произведения этих преобразований:

а) $\begin{pmatrix}1&2&3&4&5\\4&2&3&2&4\end{pmatrix}$, $\begin{pmatrix}1&2&3&4&5\\3&1&2&1&2\end{pmatrix}$;

б) $\begin{pmatrix}a&b&c&d&e\\a&b&a&b&c\end{pmatrix}$, $\begin{pmatrix}a&b&c&d&e\\c&d&c&a&b\end{pmatrix}$;

в) $\begin{pmatrix}1&2&3&4&5&6\\2&3&1&2&1&2\end{pmatrix}$, $\begin{pmatrix}1&2&3&4&5&6\\2&3&1&2&1&6\end{pmatrix}$.

3. Доказать, что произведение симметрий относительно прямых, которые пересекаются, является поворотом.

4. Преобразования φ, ψ заданы графиками. Указать правило нахождения графика $\varphi\circ\psi$.

5. Если произведение $\varphi\circ\psi$ преобразований φ, ψ конечного множества — перестановка, то φ и ψ — перестановки. Доказать это.

6. Если для заданного преобразования φ существует такое число n, что φ^n — тождественное преобразование, то φ — биекция. Доказать это (определение φ^n см. в § 6).

7. Решить уравнения:

а) $\begin{pmatrix}1&2&3&4&5&6\\6&4&3&2&1&5\end{pmatrix}\circ x=\begin{pmatrix}1&2&3&4&5&6\\3&2&1&4&5&6\end{pmatrix}$;

б) $x \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$.

8. Какие решения имеют следующие уравнения и сколько:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 3 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$;

б) $x \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 2 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$;

г) $x \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$?

9. Пусть M — произвольное множество, $\varphi: M \to M$ — некоторое преобразование M. *Правым* (*левым*) *обратным к* φ называется такое преобразование α множества M, что $\varphi \circ \alpha = \varepsilon$ (соответственно $\alpha \circ \varphi = \varepsilon$). Докажите, что преобразование φ тогда и только тогда обладает правым (левым) обратным, когда φ инъективно (соответственно сюръективно).

① ③ ⑤ ⑦   ⑧ ⑥ ④ ② ① ③ ⑤ ⑦

② ④ ⑥ ⑧

Рис. 8

10. Если φ инъективно (сюръективно), то уравнение (5) (соответственно (6)) при любом преобразовании ψ имеет решение (но, вообще говоря, не одно). Докажите это, используя упражнение 9.

11. Пусть φ сюръективно (инъективно). Докажите, что если уравнение (5) (соответственно (6)) имеет решение, то оно единственно.

12. $2n$ физкультурников выстроены в шеренгу по одному. Рассчитавшись на первого-второго, они сдваивают ряды. Стоящие во втором ряду, начиная с бывшего левофлангового, делают «обходной маневр» и переходят на правый край так, что левофланговый обращается в правофлангового (рис. 8). Считая, что номера на майках физкультурников соответствуют перед перегруппировкой их порядковым номерам в шеренге, найти перестановку, характеризующую расположение физкультурников в шеренге после трехкратной перегруппировки.

§ 4. ГРУППА ПЕРЕСТАНОВОК И ПОЛУГРУППА ПРЕОБРАЗОВАНИЙ

Как было установлено, операция умножения преобразований произвольного множества M имеет ряд свойств, которые не зависят от природы элементов множества M. Эти свойства могут быть разными для разных совокупностей преобразований множества M. Например, в множестве всех преобразований не для каждого преобразо-

вания существует обратное, а в множестве биективных преобразований это имеет место. Операция умножения произвольных преобразований некоммутативна, а операция умножения (последовательного выполнения) параллельных переносов на плоскости коммутативна. Изучать свойства отдельных классов преобразований относительно операции умножения бывает нужно очень часто. А потому удобно разработать определенную общую схему изучения таких свойств.

Кроме операции умножения преобразований, приходится иметь дело и с другими операциями, которые задаются на разных множествах. Например, рассматривается операция сложения действительных чисел, операция умножения в множестве рациональных чисел, операция возведения в степень в множестве целых чисел и т. д.

Это наводит на мысль рассмотреть общее понятие операции. Из приведенных примеров видно, что операция, заданная на некотором множестве D, произвольной паре элементов из D ставит в соответствие определенный элемент из D (результат применения операции). Например, операция сложения целых чисел паре (2, 3) ставит в соответствие число 5, а паре (—2, 1) — число —1; операция умножения перестановок на множестве {1, 2, 3} паре перестановок

$$\left(\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\ \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right)$$

ставит в соответствие перестановку

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

и т. д.

Следовательно, естественно дать такое определение:

Операцией на множестве D называется соответствие, при котором с каждой парой элементов из D сопоставлен определенный элемент этого же множества.

Операции обозначают разными символами, например $+$, $\times$, $\cdot$, $\circ$, $*$ и т. д. Если операция на множестве D обозначена символом $*$ и паре (a, b) элементов из D она ставит в соответствие элемент c, то коротко это записывают так:

$$a * b = c.$$

Элемент c называют *композицией* или, чаще, *произведением элементов* a, b, а операцию $*$ в этом случае называют

умножением (это оправдано тем, что очень часто операцию * понимают как умножение перестановок).

Примерами множеств с операциями являются множество целых чисел с операцией сложения, множество параллельных переносов на плоскости с операцией их последовательного выполнения, множество положительных действительных чисел с операцией возведения в степень (паре положительных чисел (a, b) ставится в соответствие число a^b), множество перестановок первых 100 натуральных чисел с операцией умножения перестановок.

Рассматриваются множества с операциями, которые имеют определенные свойства. Из сказанного в предыдущем параграфе вытекает, что естественно выделять две совокупности преобразований — множество всех преобразований и множество перестановок. Запишем отдельно свойства операции умножения произвольных преобразований и свойства операции умножения перестановок на множестве M. Будем обозначать совокупность всех преобразований множества M символом $P(M)$, а совокупность всех перестановок на этом множестве — символом $S(M)$.

А. Свойства операции умножения преобразований из $P(M)$.

$А_1$. *Произведение двух преобразований множества M — тоже преобразование этого множества*:

$$\text{если} \quad \varphi, \psi \in P(M), \quad \text{то и} \quad \varphi \circ \psi \in P(M).$$

Иными словами, множество $P(M)$ *замкнуто* относительно операции умножения преобразований.

$А_2$. *Операция умножения преобразований имеет свойство ассоциативности*, т. е. для каждых $\varphi, \psi, \omega \in P(M)$ справедливо равенство

$$(\varphi \circ \psi) \circ \omega = \varphi \circ (\psi \circ \omega).$$

$А_3$. *Существует единственное преобразование $\varepsilon \in P(M)$, такое, что для каждого $\varphi \in P(M)$*

$$\varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi.$$

Б. Свойства операции умножения перестановок из $S(M)$.

$Б_1$. *Если $\varphi, \psi \in S(M)$, то и $\varphi \circ \psi \in S(M)$.*

$Б_2$. *Операция умножения перестановок ассоциативна.*

$Б_3$. *Существует единственная перестановка $\varepsilon \in S(M)$, такая, что для каждой перестановки $\varphi \in S(M)$ имеем*

$$\varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi.$$

Б_4. *Для каждой перестановки* $\varphi \in S(M)$ *существует такая перестановка* $\psi \in S(M)$, *что*

$$\varphi \circ \psi = \psi \circ \varphi = \varepsilon.$$

Общая схема, по которой изучаются совокупности преобразований с операциями умножения, должна как-то учитывать серию свойств А или серию свойств Б. Это достигается введением общих понятий группы и полугруппы.

Определение. Произвольное множество D с заданной на нем операцией $*$ называется *полугруппой*, если:

а) для каждых $a, b \in D$ произведение $a * b$ принадлежит D;

б) для каждых трех элементов $a, b, c \in D$ выполняется равенство

$$(a * b) * c = a * (b * c), \tag{1}$$

т. е. операция умножения, заданная на D, ассоциативна;

в) существует такой элемент $e \in D$, что для каждого $a \in D$ имеем

$$a * e = e * a = a.$$

Элемент e называется *нейтральным* для операции $*$.

◀ Примеры. 1. Множество $\mathbf{Z}$ всех целых чисел для сложения — полугруппа.

Действительно, сумма целых чисел — снова целое число. Операция сложения целых чисел имеет ассоциативное свойство. Нейтральным элементом для операции сложения целых чисел служит число 0, потому что для каждого $a \in \mathbf{Z}$ имеем

$$a + 0 = 0 + a = a.$$

2. Множество $\mathbf{Q}^+$ всех положительных рациональных чисел для операции умножения,— полугруппа.

3. Множество преобразований $P(M)$ для операции последовательного выполнения преобразований — полугруппа.

Множество $\mathbf{R}^+$ положительных действительных чисел с заданной на нем операцией $a * b = a^b$ не будет полугруппой, так как эта операция не ассоциативна, т. е. для чисел из $\mathbf{R}^+$ не всегда выполняется равенство (1). Например,

$$(2 * 3) * 2 \neq 2 * (3 * 2)$$

(потому что $(2^3)^2 = 64$, а $2^{3^2} = 512$). ▶

Определение. Множество D с заданной на нем операцией $*$ называется *группой*, если удовлетворяются требования а) — в) определения полугруппы и, кроме того, такое требование:

г) для каждого элемента $a \in D$ существует такой элемент $b \in D$, что

$$a * b = b * a = e.$$

◀ Примеры. 4. Множество $\mathbf{Z}$ всех целых чисел для операции сложения — группа.

Действительно, в примере 1 было проверено выполнение требований а) — в). Кроме того, для каждого числа $a \in \mathbf{Z}$ существует такое число $b \in \mathbf{Z}$ (противоположное к а), что $a + b = b + a = 0$. Следовательно, выполняется и последнее требование определения группы.

5. Множество $\mathbf{R}^+$ положительных действительных чисел для операции умножения — группа.

Действительно, произведение положительных чисел — снова положительное число; операция умножения чисел ассоциативна; нейтральным элементом является число 1; для каждого числа $a \in \mathbf{R}^+$ существует обратное к нему число a^{-1}.

6. Множество всех поворотов плоскости вокруг фиксированной точки на произвольные углы для операции последовательного выполнения поворотов — группа.

Действительно, произведение поворотов плоскости вокруг точки O на углы α и β является поворотом вокруг этой точки или на угол $\alpha + \beta$, или на угол $|\alpha - \beta|$; операция умножения поворотов ассоциативна, так как таковой является операция умножения произвольных преобразований; нейтральный элемент — тождественное преобразование плоскости, которое можно рассматривать как поворот вокруг точки O на 0 радианов; обратным к повороту на угол α будет поворот на угол $-\alpha$. ▶

Совокупность $S(M)$ всех перестановок на множестве $M = \{1, 2, 3, \ldots, n\}$ для операции умножения перестановок образует группу. Эта группа называется *симметрической группой перестановок на множестве* M. Выполнение всех требований определения группы вытекает из свойств $Б_1 - Б_4$.

Каждая группа будет также и полугруппой, но не наоборот. Например, множество целых неотрицательных чисел для действия сложения — полугруппа, но не группа.

Операции сложения и умножения чисел имеют свойство коммутативности. Однако требование коммутативности не включено в определение полугруппы и группы. Это объясняется тем, что операция умножения преобразований не коммутативна, а исторически понятие группы возникло именно на основе изучения свойств операции умножения перестановок на конечных множествах (понятие полугруппы появилось значительно позднее). Отдельно рассматриваются группы, для которых выполняется требование коммутативности. Они называются *абелевыми* (в честь норвежского математика Н. Г. Абеля (1802—1829), установившего роль таких групп в теории разрешимости алгебраических уравнений в радикалах).

Для множеств с заданными на них операциями проверять выполнение свойств группы бывает довольно трудно. Если множество конечно, для такой проверки можно воспользоваться так называемой *таблицей умножения группы*. Эту таблицу составляют подобно таблице умножения целых чисел. Строят ее так. Пусть

$$g_1, g_2, \ldots, g_n$$

— все элементы группы G. Запишем их в первом ряду и в первом столбце подготовленной таблицы.

Затем заполним клетки таблицы, записывая в них произведения соответствующих элементов первого ряда и первого столбца в указанном порядке. В результате получим

	g_1	g_2	...	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	...	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	...	$g_2 * g_n$
⋮	⋮	⋮	...	⋮
g_n	$g_n * g_1$	$g_n * g_2$	...	$g_n * g_n$

◄ Примеры. 7. Пусть G — множество перестановок

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Непосредственно перемножая их, легко убеждаемся, что таблица умножения элементов из G будет такая:

	α_1	α_2	α_3
α_1	α_1	α_2	α_3
α_2	α_2	α_3	α_1
α_3	α_3	α_1	α_2

8. Пусть H — множество преобразований

$$\varepsilon=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\quad \alpha=\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & 1\end{pmatrix},\quad \beta=\begin{pmatrix}1 & 2 & 3\\ 2 & 2 & 2\end{pmatrix},\quad \gamma=\begin{pmatrix}1 & 2 & 3\\ 3 & 3 & 3\end{pmatrix}.$$

Перемножая эти преобразования получим такую таблицу:

	ε	α	β	γ
ε	ε	α	β	γ
α	α	α	β	γ
β	β	α	β	γ
γ	γ	α	β	γ

Пользуясь двумя последними таблицами, легко убедиться, что множества G и H для операции умножения преобразований образуют соответственно группу и полугруппу. Убедимся, например, что G — группа. Поскольку все клетки первой из отмеченных таблиц заполнены только символами α_1, α_2, α_3, множество G замкнуто относительно умножения заданных перестановок. Условие ассоциативности для умножения элементов из G выполняется автоматически, потому что оно выполняется для умножения произвольных преобразований. Перестановка α_1 является нейтральным элементом группы. Из таблицы также видно, что каждый из элементов α_1, α_2, α_3 имеет обратный, а именно $\alpha_1^{-1}=\alpha_1$, $\alpha_2^{-1}=\alpha_3$, $\alpha_3^{-1}=\alpha_2$. ▶

Упражнения

1. Образуют ли полугруппы такие множества с заданными на них операциями:

а) множество натуральных чисел с операцией, которая каждой паре чисел ставит в соответствие их наибольший общий делитель;

б) множество всех многочленов произвольной ненулевой степени для суперпозиции многочленов;

в) множество нечетных целых чисел для операции умножения?

2. Являются ли группами такие множества с заданными на них операциями:

а) множество действительных чисел для операции умножения;

б) совокупность функций $y=x$, $y=-x$, $y=1/x$, $y=-1/x$, определенных на множестве действительных чисел без нуля, для суперпозиции функций;

в) множество функций $y=x$, $y=-x$ для суперпозиции функций;

г) множества с операциями из упражнения 1?

3. Доказать, что в каждом ряду и в каждом столбце таблицы умножения для группы перестановок обозначение каждой из перестановок встречается точно два раза.

4. Какое свойство таблиц умножения абелевой группы не имеет места для таблиц умножения неабелевых групп?

5. Составить таблицу умножения:

а) для группы $S(M)$, где $M=\{1, 2, 3\}$;

б) для группы из упражнения 2, б);

в) для полугруппы $P(M)$, где $M=\{1, 2\}$.

6. Сколько можно составить разных таблиц умножения для четырехэлементного множества перестановок, которые были бы таблицами группы?

§ 5. ГРАФЫ ПРЕОБРАЗОВАНИЙ. ОРБИТЫ. ЦИКЛИЧЕСКАЯ ФОРМА ЗАПИСИ ПЕРЕСТАНОВОК

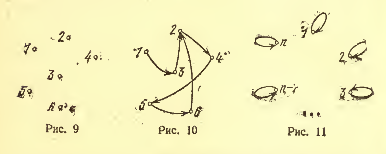
Стрелочные схемы — графы преобразований заданного множества — можно строить иначе, чем схемы произвольных отображений. Обозначим каждый элемент множества M точкой на плоскости так, чтобы разным элементам отвечали разные точки. Точки обозначим теми же самыми символами, что и соответствующие элементы множества M. Две точки соединим стрелкой в направлении от a к b тогда и только тогда, когда для элементов a, b выполняется условие $(a)\varphi=b$. Так получим *граф преобразования* φ. Ясно, что он определяет преобразование однозначно. Наоборот, если не обращать внимание на форму стрелок и размещение точек на плоскости, то каждому преобразованию будет отвечать вполне определенный граф.

◀ Примеры. 1. Пусть преобразование φ множества $M=\{1, 2, 3, 4, 5, 6\}$ задано таблицей

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 4 & 2 & 5 & 6 & 2\end{pmatrix}.$$

Обозначим каждое число из M точкой на плоскости, например, так, как на рис. 9. Поскольку $(1)\varphi = 3$, точки 1 и 3 соединим стрелкой в направлении от точки 1 к точке 3. Аналогично построим стрелки, которые выходят из точек 2, 3, 4, 5, 6 (рис. 10). Это и есть граф преобразования φ.

2. Пусть $\varphi = \varepsilon$ — тождественное преобразование множества $M = \{1, 2, 3, \ldots, n\}$. По определению, для каждого $a \in M$ $(a)\varepsilon = a$. Так что граф преобразования ε будет такой, как на рис. 11.

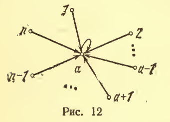

Рис. 9 Рис. 10 Рис. 11

3. Пусть $\varphi = \psi_a$ — постоянное преобразование множества $M = \{1, 2, \ldots, n\}$, которое каждому элементу $b \in M$ ставит в соответствие фиксированный элемент $a \in M$, т. е. для каждого $b \in M$ имеем

$$(b)\psi_a = a.$$

В этом случае на графе преобразования φ каждая точка b соединена с фиксированной точкой a стрелкой, которая заканчивается в a (рис. 12).

4. Пусть $M = \mathbf{Z}$, φ — преобразование множества $\mathbf{Z}$, которое каждому целому числу x ставит в соответствие число $x + 3$: $(x)\varphi = x + 3$. В этом случае граф преобразования полностью построить не удается, но можно изобразить определенную часть его так, чтобы стало понятным строение графа в целом (рис. 13).


Рис. 12

5. Если M — конечное множество и преобразование φ является перестановкой на множестве M, то из каждой вершины графа φ выходит одна и только одна стрелка и в каждую вершину обязательно входит стрелка, причем только одна.

В частности, если $M=\{1, 2, 3, 4, 5, 6, 7\}$ и φ — перестановка на множестве M:

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 2 & 4 & 1 & 3 & 6 & 5 & 7\end{pmatrix},$$

то ее граф будет такой, как на рис. 14. ▶

Граф произвольного преобразования φ состоит из одной (рис. 10, 12) или нескольких (рис. 14) не связанных между собой частей, каждая из которых составляет одно целое. При этом отдельная связная часть графа преобразования φ может состоять лишь из одной точки с «петлей», т. е. со стрелкой, которая выходит из этой точки

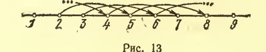


Рис. 13

и заканчивается в ней. Если a — такая точка, то для соответствующего элемента $a \in M$ справедливо равенство

$$(a)\varphi = a.$$

Такие элементы называются *неподвижными точками преобразования* φ. Если для элемента $a \in M$ выполняется условие

$$(a)\varphi \neq a,$$

то a называется *подвижной точкой преобразования* φ. На графе подвижные точки— это точки без петель.

Например, на рис. 14 точки $1, 2, 3, 4, 5, 6$ — подвижные, а точка 7 — неподвижная точка преобразования φ.

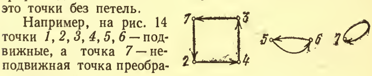


Рис. 14

Количество подвижных точек преобразования является одной из важных его характеристик, которая называется *степенью* этого преобразования. Единственным преобразованием степени нуль является тождественное преобразование; постоянное преобразование множества из n элементов имеет степень $n-1$.

Пусть φ — некоторое преобразование множества M и a — произвольный элемент из M. Последовательность

$$a_0 = a, \quad (a)\varphi = a_1, \quad (a_1)\varphi = a_2, \ \ldots, \ (a_n)\varphi = a_{n+1}, \ \ldots \qquad (1)$$

элементов из M называется *орбитой элемента a для преобразования* φ. В общем случае множество $O(a, \varphi) = \{a_0, a_1, \ldots, a_n, \ldots\}$ элементов орбиты (1) является подмножеством множества M. В частности, может случиться, что $O(a, \varphi) = M$.

Рассмотрим детально строение орбит, когда M — конечное множество, $O(a, \varphi) = M$ и $|M| = m$. Очевидно, в этом случае элементы в последовательности (1), начиная с некоторого места, будут повторяться. Пусть k — наименьшее число такое, что

$$(a_k)\varphi = a_l, \qquad l < k.$$

Ясно, что элементы $a_{k+1}, a_{k+2}, \ldots$ также встречаются среди элементов $a_0, a_1, a_2, \ldots, a_k$. Поэтому $k = m - 1$ и легко понять, что граф преобразования φ будет такой, как на рис. 15.

Если $l \neq 0$, преобразование φ не является перестановкой, потому что в точке a_l заканчиваются две стрелки. Для $l = 0$ преобразование имеет граф, который называется циклом (рис. 16), и в этом случае оно, очевидно, будет перестановкой. Эта перестановка действует на элементы из M так:

$$(a_0)\varphi = a_1, \quad (a_1)\varphi = a_2, \quad \ldots, \quad (a_{m-2})\varphi = a_{m-1}, \quad (a_{m-1})\varphi = a_0.$$

Такая перестановка называется *циклической* или просто *циклом* и обозначается

$$\varphi = (a_0, a_1, a_2, \ldots, a_{m-1}).$$

Число m есть *длина цикла*. Циклы длины 2 называются *транспозициями*.

Если элементы орбиты $O(a, \varphi)$ не исчерпывают все множество M, то графы (рис. 15, 16) не полностью характеризуют преобразование. Тогда нужно рассмотреть орбиты других элементов, которые не вошли в $O(a, \varphi)$. Разные орбиты для заданного преобразования могут иметь общие вершины (рис. 12), но *для перестановки разные орбиты очерчивают не связанные части ее графа.*

Действительно, пусть $O_1 = \{a_1, a_2, \ldots, a_m\}$ и $Q_2 = \{b_1, b_2, \ldots, b_n\}$ — разные орбиты перестановки φ. Допустим, что O_1 и O_2 имеют общие элементы. Идя в порядке возрастания номеров, выберем первый элемент $a_k \in O_1$, который равняется определенному элементу $b_l \in O_2$. Тогда $a_{k-1} \neq b_{l-1}$. Значит, $(a_{k-1})\varphi = a_k = b_l = (b_{l-1})\varphi$ и преобразование φ не является перестановкой. Мы

пришли к противоречию, которое и доказывает сформулированное утверждение.

Теперь можно подробнее охарактеризовать графы перестановок на конечном множестве M. В этом случае множество M распадается на отдельные части без общих элементов. На каждой из этих частей перестановка φ сбразует цикл. Поэтому граф каждой перестановки состоит из определенного числа не связанных между собой циклов.

Поскольку граф перестановки распадается на отдельные, не связанные между собой циклы, перестановки на конечном множестве удобно записывать так, чтобы по этой записи сразу же можно было строить отдельные части графа — циклы. Соответствующая запись перестановок называется *циклической*. Прежде чем рассказать про такую форму записи перестановок, сделаем несколько общих замечаний.

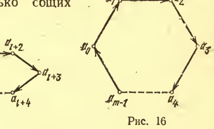


Рис. 15

Рис. 16

Пусть φ — произвольная перестановка на множестве M и P — такое подмножество множества M, что для каждого элемента $a \in P$ имеем

$$(a)\varphi \in P.$$

По перестановке φ на множестве M можно определить преобразование ψ на множестве P, положив для каждого $b \in P$

$$(b)\psi = (b)\varphi.$$

Ясно, что ψ является перестановкой на P. Будем называть ее *ограничением перестановки* φ *на подмножество* P *множества* M.

◀ Пример 6. Пусть

$$M = \{1, 2, 3, 4, 5, 6\}, \qquad P = \{1, 2, 3, 4\},$$

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}.$$

Непосредственно видно, что $(a)\varphi \in P$ для каждого $a \in P$, поэтому можно рассмотреть ограничение φ на P.

Это будет перестановка

$$\psi=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}. \blacktriangleright$$

Обратно, если имеем перестановку ψ на множестве $P\subset M$, то можно определить перестановку φ на множестве M, положив для каждого элемента $a\in M$:

$$(a)\varphi=\begin{cases}(a)\psi, & \text{если } a\in P,\\ a, & \text{если } a\notin P.\end{cases}$$

То есть на элементы из P перестановка φ действует так же, как перестановка ψ, а все остальные элементы из M оставляет на месте. Будем называть перестановку φ *расширением перестановки* ψ *на множество* M.

◀ Пример 7. Пусть

$$P=\{1, 2, 3, 4, 5\}, \qquad M=\{1, 2, 3, 4, 5, 6, 7, 8\}$$

и

$$\psi=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}.$$

Тогда расширением ψ на M является перестановка

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 3 & 1 & 5 & 4 & 6 & 7 & 8\end{pmatrix}. \blacktriangleright$$

Назовем две перестановки на множестве M *взаимно простыми*, если их множества подвижных точек не имеют общих элементов.

Взаимно простыми будут, например, перестановки

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 3 & 4 & 2 & 1 & 5 & 6 & 7 & 8\end{pmatrix}, \qquad \psi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 1 & 2 & 3 & 4 & 5 & 7 & 6 & 8\end{pmatrix},$$

ибо множеством подвижных точек для φ является $\{1, 2, 3, 4\}$, для ψ — $\{6, 7\}$.

В отличие от перестановок общего вида, *произведение взаимно простых перестановок не зависит от порядка множителей*.

Действительно, пусть φ и ψ — взаимно простые перестановки и a — произвольный элемент множества M. Если a — подвижная точка для перестановки φ, то положим $(a)\varphi=b$; элементы a, b — неподвижные точки для ψ, ибо $(a)\varphi\neq a$ и $(b)\varphi\neq b$. Поэтому имеем

$$(a)(\varphi\circ\psi)=((a)\varphi)\psi=(b)\psi=b,$$
$$(a)(\psi\circ\varphi)=((a)\psi)\varphi=(a)\varphi=b,$$

т. е. в этом случае $(a)(\varphi\circ\psi)=(a)(\psi\circ\varphi)$.

Если a — неподвижная точка перестановки φ, то положим $(a)\psi = c$ (если a является неподвижной точкой и для перестановки ψ, то $a = c$) и аналогично получим, что элементы a, c не меняются под действием перестановки φ, а поэтому

$$(a)(\varphi \circ \psi) = ((a)\varphi)\psi = (a)\psi = c,$$
$$(a)(\psi \circ \varphi) = ((a)\psi)\varphi = (c)\varphi = c.$$

Так что и в этом случае перестановки $\varphi \circ \psi$ и $\psi \circ \varphi$ действуют на элемент $a \in M$ одинаково, а это и означает, что

$$\varphi \circ \psi = \psi \circ \varphi.$$

Таблицу произведения двух взаимно простых перестановок φ, ψ составить очень просто. Для этого во втором ряду таблицы $\varphi \circ \psi$ нужно записать на своих местах (т. е. на тех местах, на которых они стоят в таблицах для φ, ψ) все подвижные точки перестановок φ, ψ, а остальные места заполнить неподвижными точками. Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \underline{3} & \underline{1} & \underline{2} & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & \underline{6} & \underline{5} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \underline{3} & \underline{1} & \underline{2} & 4 & \underline{6} & \underline{5} \end{pmatrix}.$$

Пусть теперь φ — произвольная перестановка на множестве M. Разобьем M на части $M_1, M_2, \ldots, M_s$, каждая из которых является орбитой некоторого элемента из M. Это разбиение имеет такие свойства:

а) каждый элемент из M принадлежит одному из подмножеств M_i $(i = 1, 2, \ldots, s)$;

б) если $i \neq j$, то M_i и M_j не имеют общих элементов;

в) для каждого $a \in M_i$ (i есть один из номеров $1, 2, \ldots, s$) элемент $(a)\varphi$ также принадлежит M_i.

По последнему свойству можно рассмотреть ограничение φ_i перестановки φ на каждое из подмножеств M_i; φ_i есть, очевидно, циклическая перестановка на M_i. Она определяется перестановкой φ однозначно.

В свою очередь, каждую из перестановок φ_i можно расширить на все множество M. Обозначим это расширение через $\bar{\varphi}_i$ $(i = 1, 2, \ldots, s)$. Далее такие перестановки также будем называть циклическими и обозначать их так, как и обычные циклы. Следовательно, перестановка будет циклической в этом понимании тогда и только тогда, когда она имеет граф такого вида, как на рис. 17.

Очевидно, множество подвижных точек каждой из перестановок $\bar{\varphi}_i$ совпадает с множеством M_i; по свойству в) перестановки $\bar{\varphi}_i$ и $\bar{\varphi}_j$, $i \neq j$, взаимно просты. Пользуясь приведенным выше правилом для умножения взаимно простых перестановок, получаем

$$\varphi = \bar{\varphi}_1 \circ \bar{\varphi}_2 \circ \ldots \circ \bar{\varphi}_s.$$

Поскольку перестановки $\bar{\varphi}_1, \bar{\varphi}_2, \ldots, \bar{\varphi}_s$ — попарно взаимно простые, это произведение не зависит от порядка множителей. Таким образом, доказана такая

Теорема. *Каждую перестановку на конечном множестве M можно разложить в произведение взаимно простых циклов, причем это разложение однозначно с точностью до порядка множителей.*

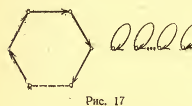


Рис. 17

Набор чисел $k_1, k_2, \ldots, k_s$, являющихся длинами циклов, на которые разложена данная перестановка, называется ее *типом* и обозначается $\langle k_1, k_2, \ldots, k_s \rangle$.

◀ Пример 8. Разложить в произведение циклов перестановку

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 6 & 7 & 4 & 5 & 8 \end{pmatrix}.$$

Находим разные орбиты для φ. Имеем

$$(1)\varphi = 2,\ (2)\varphi = 3,\ (3)\varphi = 1;\quad (4)\varphi = 6,\quad (6)\varphi = 4;$$
$$(5)\varphi = 7,\ (7)\varphi = 5,\ (8)\varphi = 8.$$

Так что орбиты определяют подмножества $\{1, 2, 3\}$, $\{4, 6\}$, $\{5, 7\}$, $\{8\}$. Ограничениями перестановки φ на эти множества будут такие перестановки:

$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\quad \varphi_2 = \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix},\quad \varphi_3 = \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix},\quad \varphi_4 = \begin{pmatrix} 8 \\ 8 \end{pmatrix}.$$

Расширениями этих перестановок на множество M будут перестановки

$$\bar{\varphi}_1 = (1,\ 2,\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 \end{pmatrix},$$

$$\bar{\varphi}_2 = (4,\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 6 & 5 & 4 & 7 & 8 \end{pmatrix},$$

$$\bar{\varphi}_3 = (5,\ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 & 8 \end{pmatrix},$$

$$\bar{\varphi}_4 = (8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \varepsilon.$$

Поэтому можно записать

$$\varphi = \bar{\varphi}_1 \cdot \bar{\varphi}_2 \cdot \bar{\varphi}_3 \cdot \bar{\varphi}_4 = (1,\ 2,\ 3) \cdot (4,\ 6) \cdot (5,\ 7) \cdot (8) = (1,\ 2,\ 3) \cdot (4,\ 6) \cdot (5,\ 7).$$

Последняя запись однозначно определяет перестановку лишь тогда, когда известно, на каком множестве она действует. ▶

Упражнения

1. Может ли произвольный граф быть графом какого-нибудь преобразования?

2. Перестановка задана графом. Как построить граф обратной перестановки?

3. Указать правило для нахождения графа произведения преобразований, каждое из которых задано своим графом, не строя таблиц этих преобразований.

4. Построить графы преобразований, заданных таблицами:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 8 & 3 & 7 & 2 & 4 \end{pmatrix}$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 5 & 4 & 3 & 7 & 1 & 3 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 3 & 7 & 5 & 1 & 2 \end{pmatrix}$; г) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 8 & 4 & 3 & 4 & 9 & 9 \end{pmatrix}$.

5. Каждая перестановка, граф которой связан, циклична. Доказать это.

6. *Длиной орбиты* называется число ее элементов. Найти наибольшее и наименьшее значения сумм длин разных орбит для преобразований множества из n элементов.

7. Преобразование φ множества M будет перестановкой тогда и только тогда, когда сумма длин разных ее орбит равняется $|M|$. Доказать это.

8. Пусть φ — произвольное преобразование множества M. Существует такое множество $P \subset M$ и такое натуральное число k, что $(a)\varphi^k \in P$ для каждого $a \in P$ и ограничение φ^k на P есть перестановка. Доказать это.

9. Разложить в произведение взаимно простых циклов и найти типы таких перестановок:

$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}, \qquad \varphi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix},$$

$$\varphi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 3 & 1 & 5 & 8 & 4 & 2 & 6 \end{pmatrix}.$$

10. Описать общий вид графа про зводьного преобразования (так, как это сделано для перестановок).

11. Сколько существует перестановок на множестве из m элементов, которые имеют заданный тип $\langle n_1, n_2, \ldots, n_k \rangle$, где $n_1 < n_2 < \ldots < n_k$ (ясно, что $n_1 + n_2 + \ldots + n_k = m$).

12. В группе $S_4 = S(\{1, 2, 3, 4\})$ найти число перестановок каждого возможного типа.

13. Определить тип перестановки, характеризующей расположение тридцати физкультурников после двукратной перегруппировки (см. упражнение 12 § 3).

§ 6. ПОРЯДОК ПЕРЕСТАНОВКИ

Для каждого преобразования φ можно рассмотреть его степени; *n-й степенью преобразования* φ называется произведение

$$\underbrace{\varphi \circ \varphi \circ \varphi \circ \ldots \circ \varphi}_{n},$$

где n — натуральное число. Далее будем обозначать его φ^n.

Из определения степени преобразования вытекают такие равенства:

$$\text{а) } \varphi^n \circ \varphi^m = \varphi^{n+m}; \quad \text{б) } (\varphi^n)^m = \varphi^{nm}.$$

Положим также для каждого преобразования φ

$$\varphi^0 = \varepsilon.$$

Для перестановок (произвольных биекций) понятие степени можно обобщить и на случай целых отрицательных чисел, положив

$$\varphi^{-n} = \underbrace{\varphi^{-1} \circ \varphi^{-1} \circ \ldots \circ \varphi^{-1}}_{n} = (\varphi^{-1})^n = (\varphi^n)^{-1}.$$

Равенства а) и б) в этом случае будут верны для произвольных целых показателей.

Если φ — некоторая перестановка на множестве M, $|M| < \infty$, то φ^n для каждого целого n также есть перестановка на M. Таких перестановок лишь конечное число, т. е. в последовательности φ, φ^2, φ^3, φ^4, ... не все перестановки разные.

Пусть для некоторых натуральных чисел k, l $(k < l)$ выполняется равенство $\varphi^k = \varphi^l$. Тогда

$$(\varphi^k)^{-1} = \varphi^{-k}, \qquad (\varphi^k)^{-1} \circ \varphi^k = (\varphi^k)^{-1} \circ \varphi^l,$$

откуда $\varphi^{l-k} = \varepsilon$, т. е. *для каждой перестановки* $\varphi \in S(M)$, *где* M — *конечное множество, найдется по меньшей мере одно натуральное число* s, *такое*, что $\varphi^s = \varepsilon$. Наименьшее из таких натуральных чисел называется *порядком перестановки* φ.

Степени циклической перестановки $(a_1, a_2, \ldots, a_n)$ находят по формуле

$$(a_1, a_2, \ldots, a_n)^k = (a_k, a_{k+1}, \ldots, a_n, a_1, \ldots, a_{k-1}).$$

Это равенство можно толковать так. Если какая-нибудь шестерня, которая имеет n зубцов, поворачивается вокруг своего центра, то, занумеровав зубцы числами

1, 2, 3, ..., n и зафиксировав некоторое начальное положение зубцов, ее повороты можно однозначно описывать перестановками на множестве $\{1, 2, \dots, n\}$. Циклическая перестановка

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix},$$

очевидно, описывает поворот на угол $2\pi/n$ (зубец с номером 1 встает на место зубца с номером 2 и т. д.).

Не нарушая общности, будем считать, что шестерня поворачивается по часовой стрелке. Чтобы повернуть шестерню на угол $2k\pi/n$, надо k раз осуществить поворот на угол $2\pi/n$ в одном направлении, так что перестановка α^k, $k > 0$, отвечает такому положению шестерни, когда на месте первого зубца стоит k-й, на месте второго $(k+1)$-й и т. д. Если шестерню повернуть n раз вокруг центра на угол $2\pi/n$, то она займет начальное положение. Таким образом, для каждого цикла $(a_1, a_2, \dots, a_n)$ выполняется равенство

$$(a_1, a_2, \dots, a_n)^n = \varepsilon.$$

При этом для натуральных чисел, меньших n, это равенство невозможно. Для $k < 0$ перестановки α^k описывают повороты шестерни на углы $2\pi k/n$ против часовой стрелки.

По доказанному в предыдущем параграфе произвольную перестановку можно разложить в произведение попарно взаимно простых циклов:

$$\varphi = \varphi_1 \circ \varphi_2 \circ \dots \circ \varphi_s.$$

Для любых номеров i, j произведение перестановок φ_i, φ_j не зависит от порядка множителей. Пользуясь этим, i-ю степень перестановки φ для каждого целого n можно записать так:

$$\varphi^n = \underbrace{(\varphi_1 \circ \varphi_2 \circ \dots \circ \varphi_s) \circ \dots \circ (\varphi_1 \circ \varphi_2 \circ \dots \circ \varphi_s)}_{n} =$$

$$= \underbrace{(\varphi_1 \circ \varphi_1 \circ \dots \circ \varphi_1)}_{n} \circ \underbrace{(\varphi_2 \circ \varphi_2 \circ \dots \circ \varphi_2)}_{n} \circ \dots \circ \underbrace{(\varphi_s \circ \varphi_s \circ \dots \circ \varphi_s)}_{n} =$$

$$= \varphi_1^n \circ \varphi_2^n \circ \dots \circ \varphi_s^n. \qquad (1)$$

Это равенство также допускает механическое толкование. Поскольку циклы $\varphi_1, \varphi_2, \dots, \varphi_s$ взаимно просты, их степени описывают повороты вокруг центров s шестеренок с соответствующими количествами зубцов, причем эти шестерни не связаны одна с другой. Поэтому степенями перестановки φ описываются повороты целой системы

шестеренок. Зубцы каждой из шестеренок можно занумеровать так, чтобы все повороты осуществлялись в одном направлении.

Порядок является очень важной характеристикой перестановки. Чисел n, таких, что $\varphi^n = \varepsilon$, для произвольной перестановки φ существует много, но *все они делятся на порядок перестановки.*

Докажем это методом от противного. Допустим, что существует такое натуральное число k, для которого справедливо равенство

$$\varphi^k = \varepsilon,$$

причем k не делится на порядок r перестановки φ. По определению порядка перестановки $k > r$, поэтому

$$k = lr + s, \qquad 0 < s < r.$$

Тогда имеем $\varphi^k = \varphi^{lr+s} = \varphi^{lr} \circ \varphi^s$. Но

$$\varphi^{lr} = (\varphi^r)^l = \varepsilon^l = \varepsilon.$$

Таким образом,

$$\varepsilon = \varphi^k = \varphi^s.$$

Однако $0 < s < r$, и мы пришли к противоречию, которое и доказывает сформулированное утверждение.

Выведем теперь правило для нахождения порядка произвольной перестановки. Прежде всего, заметим, что *произведение нескольких взаимно простых перестановок может равняться тождественной перестановке лишь тогда, когда каждая из перестановок единична.* Это вытекает из того, что произведение φ взаимно простых перестановок $\varphi_1, \varphi_2, \ldots, \varphi_s$ действует на каждую свою подвижную точку так, как действует на нее та перестановка φ_i, для которой эта точка является подвижной. Поэтому из равенства (1) получаем, что $\varphi^n = \varepsilon$ тогда и только тогда, когда одновременно

$$\varphi_1^n = \varepsilon, \quad \varphi_2^n = \varepsilon, \ \ldots, \ \varphi_s^n = \varepsilon. \tag{2}$$

Если перестановки $\varphi_1, \varphi_2, \ldots, \varphi_s$ есть циклы длины $k_1, k_2, \ldots, k_s$ соответственно, т. е. имеют порядки $k_1, k_2, \ldots$ $\ldots, k_s$, то наименьшее число n, для которого одновременно выполняются все равенства (2), равняется, очевидно, наименьшему общему кратному чисел $k_1, k_2, \ldots, k_s$. Следовательно, мы доказали, что порядок перестановки φ, которая раскладывается в произведение циклов длиною $k_1, k_2, \ldots, k_s$ есть наименьшее общее кратное чисел

$k_1, k_2, \ldots, k_s$.

$$\text{пор. } \varphi = K(\text{пор. } \varphi_1, \text{ пор. } \varphi_2, \ldots, \text{ пор. } \varphi_s).$$

◀ Пример. Пусть

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 7 & 2 & 5 \end{pmatrix}.$$

Разложим φ в произведение циклов:

$$\varphi = (1, 3, 4) \circ (2, 6, 7) \circ (5, 8).$$

Отсюда пор. $\varphi = K(3, 3, 2) = 6$. ▶

Упражнения

1. Найти порядок каждой из перестановок:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 9 & 6 & 8 & 1 & 2 & 4 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 7 & 8 & 9 & 2 & 1 & 10 \end{pmatrix}$.

2. Найти порядки всех перестановок на множестве из 6 элементов.

3. Какой наивысший порядок могут иметь перестановки на множестве из 10 элементов?

4. Найти перестановку, обратную к циклу $(a_1, a_2, \ldots, a_n)$.

5. Если произведение перестановок φ и ψ не зависит от порядка записи множителей, то порядок $\varphi \circ \psi$ есть делитель наименьшего общего кратного порядков φ и ψ. В общем случае нельзя утверждать, что пор. $(\varphi \circ \psi) = K$ (пор. φ, пор. ψ). Привести примеры.

6. Сколько существует перестановок 15-го порядка на множестве из 8 элементов?

7. Вывести формулу для нахождения порядка перестановки, пользуясь механическим толкованием действия возведения в степень.

8. Если n — простое число, то для каждого k, $0 < k < n$, перестановка $(a_1, a_2, \ldots, a_n)^k$ есть цикл длины n. Если число n — составное, то эта перестановка будет циклом для чисел k, взаимно простых с n, и произведением циклов одинаковой длины в ином случае. Доказать это.

9. Доказать, что для каждой перестановки φ, которая раскладывается в произведение l циклов одинаковой длины s, найдется цикл ψ длины ls и натуральное число k, такое, что $\varphi = \psi^k$. Единственный ли такой цикл?

10. 12 мальчиков перебрасываются разноцветными мячами, каждый из них бросает свой мяч всегда одному и тому же партнеру, все мячи бросаются одновременно, и никакие два мальчика не бросают мяч одному игроку. Через какое наименьшее число ходов игры все мячи окажутся в руках тех же мальчиков, что и в начале?

11. Колода из 36 карт тасуется следующим образом. Колода берется лицевой стороной вниз в левую руку и карты сверху по одной перекладываются в правую руку, причем в правой руке они поочередно кладутся то сверху, то снизу тех карт, которые к этому моменту уже скопились в правой руке. Сколько раз нужно повторить такую перетасовку, чтобы в колоде был восстановлен первоначальный порядок?

12. Какое наименьшее число перегруппировок тридцати физкультурников (см. упр. 12 § 3) нужно осуществить, чтобы в шеренге был восстановлен начальный порядок? Какой ответ получится в случае, когда физкультурников 36?

§ 7. ОБРАЗУЮЩИЕ СИММЕТРИЧЕСКОЙ ГРУППЫ

Задача. На стенах круглого зала картинной галереи висели картины. Как-то решили разместить их в другом порядке, меняя местами картины, которые висят рядом. Всегда ли можно с помощью таких перемещений разместить картины, как задумано?

Решение. Занумеруем картины в первоначальном порядке числами 1, 2, ..., n. Пусть на место первой картины нужно повесить картину с номером i_1, на место второй — картину с номером i_2 и т. д., наконец, на место n-й картины — картину с номером i_n (i_1, i_2, ..., i_n — разные числа из множества $\{1, 2, \ldots \ldots, n\}$). Перемещаясь вдоль стены обозначенным способом в одном направлении картины последовательно занимает все места, на которых висят картина. Поэтому картину с номером i_1 можно повесить на место первой картины (рис. 18). Выбирая направление перемещения картины с номером i_2 так, чтобы не двигать картину с номером i_1, картину с номером i_2 можно повесить на место второй. Аналогично, выбирая такое направление перемещения, чтобы не двигать картины с номерами i_1 и i_2, картину с номером i_3 можно повесить на место третьей. Продолжая этот процесс дальше, каждую картину можно повесить на нужное место. Следовательно, ответ на вопрос, поставленный в задаче, утвердительный.

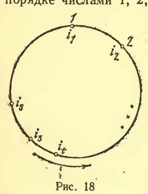


Рис. 18

Сформулируем теперь эту задачу на языке перестановок. Занумеруем места, на которых висят картины, так, чтобы нумерация мест совпадала с нумерацией картин в первоначальном положении. Размещение картин, при котором картина с номером i_1 висит на первом месте, картина с номером i_2 — на втором и т. д., картина с номером i_n — на n-м месте, однозначно описывается перестановкой

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}, \qquad (1)$$

в частности, первоначальное размещение картин характеризуется тождественной перестановкой. Если в положении, которое описывается перестановкой (1), поменять местами картины, которые стоят на k-м и $(k+1)$-м местах $(1 \leqslant k \leqslant n)$, то перестановка α_1, которая будет характеризовать это новое положение, будет результатом умножения перестановки α слева на транспозицию $(k, k+1)$:

$$\begin{pmatrix} 1 & 2 & \dots & k-1 & k+1 & k & k+2 & \dots & n \\ i_1 & i_2 & \dots & i_{k-1} & i_k & i_{k+1} & i_{k+2} & \dots & i_n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & k+2 & \dots & n \\ 1 & 2 & \dots & k-1 & k+1 & k & k+2 & \dots & n \end{pmatrix} \circ$$

$$\circ \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & k+2 & \dots & n \\ i_1 & i_2 & \dots & i_{k-1} & i_k & i_{k+1} & i_{k+2} & \dots & i_n \end{pmatrix}.$$

Если переход от первоначального положения к желаемому, которому отвечает перестановка φ, осуществляется за s шагов, то можно записать

$$\delta_1 \circ \delta_2 \circ \dots \circ \delta_s \circ \varepsilon = \varphi,$$

где $\delta_1, \delta_2, \dots, \delta_s$ — некоторые транспозиции. Следовательно, вопрос задачи можно сформулировать так: можно ли разложить произвольную перестановку в произведение транспозиций?

Аналогичные вопросы интересно решать не только для транспозиций, но и для произвольных множеств перестановок.

Определение. Подмножество T множества всех перестановок называется *системой образующих симметрической группы* S, если каждую перестановку из S можно разложить в произведение перестановок из T.

В § 5 было установлено, что системой образующих является совокупность всевозможных циклов. Каждый цикл $(a_1, a_2, \dots, a_s)$ можно разложить в произведение транспозиций:

$$(a_1, a_2, \dots, a_s) = (a_1, a_2) \circ (a_1, a_3) \circ \dots \circ (a_1, a_s)$$

(проверьте!). Пользуясь этим, каждую перестановку, разложив ее сначала в произведение циклов, можно представить в виде произведения транспозиций.

◀ Пример 1. Разложить в произведение транспозиций перестановку

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}.$$

Раскладываем φ в произведение циклов:

$$\varphi=(1,\ 8,\ 4)\circ(2,\ 7,\ 3)\circ(5,\ 6).$$

Далее, имеем

$$(1,\ 8,\ 4)=(1,\ 8)\circ(1,\ 4),$$
$$(2,\ 7,\ 3)=(2,\ 7)\circ(2,\ 3).$$

Следовательно,

$$\varphi=(1,\ 8)\circ(1,\ 4)\circ(2,\ 7)\circ(2,\ 3)\circ(5,\ 6).\ \blacktriangleright$$

Из этого примера видно, что в разложении перестановки в произведение транспозиций порядок множителей является существенным.

Далее, будем обозначать символом S_n симметрическую группу перестановок на множестве $M=\{1,\ 2,\ \ldots,\ n\}$. В этой группе будем выделять системы образующих, которые будут состоять только из транспозиций определенного вида. Например, последовательности транспозиций

I $(1,\ 2),\ (2,\ 3),\ (3,\ 4),\ \ldots,\ (n-1,\ n)$,

II $(1,\ 2),\ (1,\ 3),\ (1,\ 4),\ \ldots,\ (1,\ n)$,

как легко убедиться, будут системами образующих для S_n. Действительно, перестановку $(i,\ j)$ можно разложить в произведение транспозиций системы II так:

$$(i,\ j)=(1,\ i)\circ(1,\ j)\circ(1,\ i). \qquad (2)$$

(Убедитесь, что перестановки, которые стоят справа и слева в этом равенстве, одинаково действуют на каждый элемент из M.) Поскольку любую перестановку φ можно разложить в произведение транспозиций вида $(i,\ j)$, то, заменив в этом разложении все транспозиции в соответствии с равенством (2), получим разложение φ в произведение транспозиций системы II.

В свою очередь, произвольную транспозицию из последовательности II можно разложить в произведение перестановок системы I по равенству

$$(1,\ k)=(1,\ 2)\circ(2,\ 3)\circ\ldots\circ(k-1,\ k)\circ(k-1,\ k-2)\circ\ldots\circ(2,\ 1). \quad (3)$$

Проверим, правильно ли равенство (3). Пусть $\delta_i=(i,\ i+1)$. Перестановка $\varphi=\delta_1\circ\delta_2\circ\ldots\circ\delta_{k-1}\circ\delta_{k-2}\circ\ldots\circ\delta_1$ действует на элементы 1 и k так:

$$1\xrightarrow{\delta_1}2\xrightarrow{\delta_2}3\xrightarrow{\delta_3}\ldots\xrightarrow{\delta_{k-1}}k\xrightarrow{\delta_{k-2}}k\xrightarrow{\delta_{k-3}}\ldots\xrightarrow{\delta_1}k,$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\varphi}$$

$$k\xrightarrow{\delta_1}k\xrightarrow{\delta_2}k\xrightarrow{\delta_3}\ldots\xrightarrow{\delta_{k-2}}k\xrightarrow{\delta_{k-1}}k-1\xrightarrow{\delta_{k-2}}\ldots\xrightarrow{\delta_1}1.$$

Остальные элементы множества будут неподвижными точками для φ. Следовательно, ряд I также есть система образующих для S_n.

Наиболее интересными системами образующих являются такие, из которых нельзя выбросить ни одной перестановки, чтобы новая система снова была системой образующих. Эти системы называются *неприводимыми*. Они могут состоять из разного количества перестановок. В частности, существуют системы образующих, которые состоят из двух перестановок (они всегда неприводимы). Например, такой будет система

$$\text{III} \quad \alpha=(1,\ 2), \quad \beta=(1,\ 2,\ 3,\ \ldots,\ n).$$

Действительно, если $1 \leqslant j \leqslant n-2$, то $(1)\beta^j=j+1$, $(2)\beta^j=j+2$, а поэтому

$$\beta^j \circ \alpha \circ (\beta^j)^{-1}=(j+1,\ j+2).$$

Таким образом, каждая перестановка системы I раскладывается в произведение перестановок α, β, потому что элемент β^j имеет конечный порядок, например l, так что $(\beta^j)^{-1}=(\beta^j)^{l-1}$.

В общем случае описать все неприводимые системы образующих симметрической группы S_n не удается. Но неприводимые системы образующих S_n, целиком состоящие из транспозиций, описываются достаточно просто.

В § 5 было введено понятие графа как совокупности точек на плоскости, некоторые из которых соединены стрелками. Такие графы называют *ориентированными*, поскольку на стрелку, соединяющую две точки, можно смотреть как на путь с фиксированной ориентацией, которая указывается направлением стрелки. Вдоль такого отрезка разрешается проходить только в одном направлении — в том, которое указано стрелкой. Здесь нам понадобится понятие неориентированного графа, которое введем следующим образом.

Неориентированным графом называется множество как угодно размещенных на плоскости точек, некоторые из которых соединены линиями любой формы. Два неориентированных графа считаются неразличимыми, если они отличаются друг от друга только формой соединительных линий или способом размещения точек на плоскости.

Выбранные на плоскости точки называются *вершинами графа*, а соединяющие их линии — его *ребрами*. Примеры неориентированных графов приведены на рис. 19. Последовательность ребер графа, в которой любые два соседние

ребра имеют общую вершину, называются *путем* в графе. Граф *связан*, если любые две вершины этого графа соединены по крайней мере одним путем. Мы рассматриваем *графы без петель*, т. е. без ребер, которые начинаются и заканчиваются в одной вершине. Такой граф называется *деревом*, если в нем нет замкнутых путей. Деревом является, например, граф, изображенный на рис. 19б, а графы 19а, в — деревьями не являются.

Пусть T_n — множество всех транспозиций из S_n. Каждая транспозиция $(i, j) \in T_n$ — это перестановка, оставляющая на месте все элементы множества $\{1, 2, \ldots, n\}$, кроме чисел i, j, которые она переставляет. Поэтому первый элемент такой пары может быть любым из чисел $1, 2, \ldots, n$, а второй — любым отличным от первого. Итак, имеется ровно n возможностей для выбора первого элемента пары, определяющей транспозицию, и, при каждом фиксированном выборе первого элемента, $n-1$ возможность для выбора второго. Таким образом, можно построить $n(n-1)$ различных пар (i, j), определяющих транспозиции. Однако пары (i, j) и (j, i), $i \neq j$, определяют одну и ту же транспозицию, т. е. $|T_n| = n(n-1)/2$.

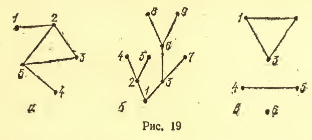


Рис. 19

Пусть A — некоторое множество транспозиций из S_n^1, т. е. $A \subset T_n$. По множеству A строится неориентированный граф, вершины которого обозначены числами $1, 2, \ldots, n$, причем вершины i, j соединены ребром тогда и только тогда, когда транспозиция (i, j) принадлежит множеству A. Например, множеству транспозиций (1, 2), (2, 3), (2, 5), (3, 5), (4, 5) соответствует граф, изображенный на рис. 19а, а множеству (1, 2), (1, 3), (2, 3), (4, 5) — граф, изображенный на рис. 19в. Граф, построенный по некоторому множеству A транспозиций, часто называют *графом Пойа* этого множества. Множества транспозиций, являющиеся системами образующих симметрической группы (приводимыми или нет), выделяются по

свойствам своих графов Пойа. Прежде чем сформулировать теорему, характеризующую системы образующих транспозиций для симметрических групп, докажем одно вспомогательное утверждение, усиливающее равенство (3).

Лемма. *Для произвольной последовательности $l_0, l_1, \ldots, l_k$ различных натуральных чисел, таких, что $l_0=i$, $l_k=j$, имеет место следующее разложение транспозиции (i, j):*

$$(i, j)=(i, l_1)\circ(l_1, l_2)\circ\ldots\circ(l_{k-1}, j)\circ(l_{k-1}, l_{k-2})\circ\ldots\circ(l_1, i). \quad (4)$$

Доказательство. Как и при проверке равенства (3), покажем, что перестановки из правой и левой частей равенства (4) действуют на любой элемент множества M одинаково. Пусть $\delta_i=(l_{i-1}, l_i)$. Тогда $(i)\delta_1=l_1$, $(l_1)\delta_2=l_2$ и т. д. На k-м шаге получим $(l_{k-1})\delta_k=j$. Действуя на элемент j любой из транспозиций $\delta_{k-1}, \delta_{k-2}, \ldots, \delta_1$, получим тот же элемент. Таким образом, перестановка, стоящая в правой части равенства (4), элемент i переводит в элемент j. Для элемента j получаем равенства $(j)\delta_1=j, \ldots, (j)\delta_{k-1}=j$, $(j)\delta_k=l_{k-1}$, $(l_{k-1})\delta_{k-1}=l_{k-2}, \ldots, (l_1)\delta_1=i$, т. е. элемент j этой подстановкой переводится в i. Пусть теперь $r\neq i, j$. Транспозиция (i, j) оставляет элемент r на месте. Если $r\notin\{l_0, l_1, \ldots, l_k\}$, то все транспозиции δ_i $(1\leqslant i\leqslant k)$ также оставляют r на месте и, следовательно, этот элемент является неподвижной точкой для перестановки из правой части (4). Если r совпадает с каким-то элементом l_s, $s\neq 0, k$, то имеем следующие равенства: $(l_s)\delta_1=l_s, \ldots, (l_s)\delta_{s-1}=l_s$, $(l_s)\delta_s=l_{s-1}$, $(l_{s-1})\delta_{s+1}=l_{s-1}, \ldots, (l_{s-1})\delta_s=l_s$, $(l_s)\delta_{s-1}=l_s, \ldots, (l_s)\delta_1=l_s$, т. е. элемент l_s является неподвижной точкой подстановки правой части из (4). Лемма доказана.

Теорема. *Множество транспозиций будет системой образующих симметрической группы S_n тогда и только тогда, когда граф Пойа этого множества связан. Система образующих симметрической группы будет неприводимой тогда и только тогда, когда граф Пойа этой системы является деревом.*

Доказательство. Пусть A — множество транспозиций, граф Пойа которого является связным, т. е. для произвольных вершин i, j этого графа $(1\leqslant i, j\leqslant n, i\neq j)$ существует путь, соединяющий эти вершины. Пусть $l_0=i$, $l_1, \ldots, l_{k-1}$, $l_k=j$ — последовательность вершин, встречающихся вдоль этого пути при прохождении от вершины i к вершине j. Согласно определению графа Пойа, подмножество A содержит транспозиции (i, l_1), $(l_1, l_2), \ldots, (l_{k-1}, j)$.

Но тогда, по доказанной выше лемме, транспозиция (i, j) раскладывается в произведение этих транспозиций из A. Поскольку вершины i, j выбраны произвольно, отсюда получаем, что любая транспозиция из T_n раскладывается в произведение транспозиций из A. Так как T_n порождает S_n, то A является системой образующих этой группы.

Предположим теперь, что граф Пойа множества A несвязан. Тогда его можно разбить на связные части, т. е. выделить подмножества таких вершин, которые в этом графе связаны между собой, а вершины из различных подмножеств между собой никак не связаны. Множество M можно представить как объединение попарно не пересекающихся частей:

$$M = M_1 \cup M_2 \cup \ldots \cup M_r,$$

причем в множество A входят лишь такие транспозиции (i, j), для которых при некотором k элементы i, j одновременно содержатся в M_k. Поэтому множество A можно разбить на r подмножеств $A_1, A_2, \ldots, A_r$ (некоторые из которых могут быть пустыми), включая в подмножество A_k те и только те транспозиции (i, j), для которых $i, j \in M_k$. Произведение транспозиций из множества A_k $(1 \leqslant k \leqslant r)$ — это некоторая перестановка на множестве M, подвижные точки которой принадлежат M_k. Так как $M_1, M_2, \ldots, M_r$ попарно не пересекаются, то при любых i, j, $i \neq j$, перестановки, порождаемые транспозициями из A_i и A_j, являются взаимно простыми. Итак, любую перестановку φ, которая раскладывается в произведение транспозиций из множества A, можно разложить в произведение

$$\varphi = \varphi_1 \circ \varphi_2 \circ \ldots \circ \varphi_r$$

перестановок $\varphi_1, \varphi_2, \ldots, \varphi_r$, подвижные точки которых содержатся соответственно в множествах $M_1, M_2, \ldots, M_r$. Поскольку произвольную перестановку из S_n (например, цикл длины n) в таком виде записать нельзя, множество A транспозиций системой образующих S_n не является.

Каждый граф, являющийся деревом, будет связным. Поэтому множество транспозиций A, граф Пойа которого является деревом, будет системой образующих группы S_n. Поскольку при выбрасывании из дерева любого ребра его связность нарушается, такое множество транспозиций A является неприводимой системой образующих симметрической группы.

С другой стороны, если граф Пойа множества транспозиций A деревом не является, то в нем можно выбрать

последовательность $l_0, l_1, \ldots, l_k, l_{k+1}=l_0$ вершин так, что соединяющие их ребра образуют замкнутый путь. Транспозиции $(l_0, l_1), (l_1, l_2), \ldots, (l_{k-1}, l_k), (l_k, l_0)$ содержатся в множестве A по определению графа Пойа. Поскольку числа $l_0, l_1, \ldots, l_k$ удовлетворяют условиям леммы, транспозиция (l_0, l_k) раскладывается в произведение остальных транспозиций этой последовательности. Следовательно, ее можно убрать из множества A, и оставшееся множество транспозиций будет системой образующих S_n. Таким образом, множество A неприводимой системой образующих группы S_n не является. Теорема полностью доказана.

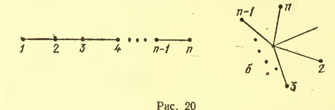


Рис. 20

Неприводимые системы образующих, целиком состоящие из транспозиций, называют *базисами* симметрической группы S_n. Поскольку графы Пойа систем I и II, приведенных на с. 52, являются деревьями (рис. 20), то эти системы неприводимы. По виду графов Пойа базис I называется *линейным базисом*, а базис II — *звездообразным*. Оба эти базиса состоят из $n-1$ транспозиции. Это не случайно. Покажем, что любое дерево с n вершинами содержит $n-1$ ребро.

Воспользуемся методом математической индукции по числу n. Случай $n=2$ — база индукции. В этом случае имеется лишь одно дерево, и оно имеет одно ребро. Предположим, что любое дерево с $k<n$ вершинами содержит $k-1$ ребро, и рассмотрим произвольное дерево с n вершинами. В любом дереве имеется по крайней мере одна «висячая» вершина, т. е. такая, которая соединена ребром только с одной вершиной дерева. (Если в конечном графе нет «висячих» вершин, то в нем обязательно есть замкнутые пути.) Удалим из дерева эту вершину и ребро, из нее выходящее. Получим снова связный граф, являющийся деревом. Поскольку число вершин этого графа равно $n-1$, к нему применимо предположение индукции, т. е. он содержит $n-2$ ребра. Следовательно, исходное дерево содержит $n-1$ ребро. Из этого простого утверждения получаем следующий важный вывод о базисах симметри-

ческой группы S_n: все базисы симметрической группы S_n равномощны и состоят из $n-1$ транспозиции.

Известна формула, принадлежащая А. Кэли[1]), для числа различных деревьев с n вершинами и, следовательно, для числа различных базисов симметрической группы S_n. Это число очень быстро растет с ростом n, т. е. при больших n в S_n имеется очень много неприводимых систем образующих (см. упражнения).

Упражнения

1. Доказать, что все перестановки из симметрической группы S_n можно расположить в такую последовательность, что:

а) все члены этой последовательности различны;

б) при любом $i=2, 3, \ldots, n!$ i-й член последовательности получается из $(i-1)$-го ее члена умножением на некоторую транспозицию.

2. Системой образующих полугруппы $P(M)$ всех преобразований множества M назовем такое множество A преобразований, что любой элемент из $P(M)$ можно разложить в произведение преобразований из A. Пусть A' — некоторая система образующих симметрической группы $S(M)$. Тогда множество $A' \cup \{\alpha\}$, где

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 1 & 3 & 4 & \ldots & n \end{pmatrix},$$

является системой образующих полугруппы $P(M)$. Доказать это.

3. Разложить перестановки

$$\text{а)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 7 & 5 & 6 & 1 & 8 \end{pmatrix}, \quad \text{б)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 1 & 4 & 3 & 5 \end{pmatrix},$$

$$\text{в)} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$$

в произведение элементов каждой из систем образующих вида I, II, III (с. 52) групп S_8, S_7 и S_6 соответственно.

4. Нужно соединить n городов автомобильными дорогами так, чтобы из одного города всегда можно было проехать в другой. Какое наименьшее число дорог надо построить?

5. Доказать, что связный граф является деревом тогда и только тогда, когда в нем для любых двух вершин существует единственный путь, соединяющий эти вершины.

6. Пусть D — дерево с множеством вершин $1, 2, \ldots, n$. Обозначим через b_1 висячую вершину дерева D, которая первой встретится в списке $1, 2, \ldots, n$, а через a_1 — вершину, которая соединена ребром с b_1. Выбрасывая из дерева D вершину b_1 и ребро, соединяющее вершины b_1 и a_1, получим дерево D_1, по которому аналогично определяются вершины b_2 и a_2. Продолжая этот процесс $n-2$ шага, получим последовательность вершин $a_1, a_2, \ldots, a_{n-2}$ дерева D. Доказать, что набор $\sigma(D) = [a_1, a_2, \ldots, a_{n-2}]$ однозначно определяет дерево D.

[1]) А. Кэли (1821—1895) — английский математик, получивший фундаментальные результаты по различным разделам алгебры и комбинаторики.

7. Используя упражнение 6, доказать, что существует в точности n^{n-2} различных деревьев с n вершинами (а следовательно, и базисов транспозиций).

8. Нужно соединить n городов линиями электропередач так, чтобы не строить лишних линий. Сколькими способами можно построить такую систему энергоснабжения?

9. Будет ли системой образующих симметрической группы S_{2n-1} совокупность транспозиций вида $(k, k+1)$, $(k, k+2)$, где k пробегает все нечетные числа от 1 до $2n-3$? Если да, то будет ли эта система неприводимой?

10. Порождает ли система $3n$ транспозиций вида $(1+3l, 1+3l+1)$, $(1+3l, 1+3l+2)$, $(1+3l, 1+3(l+1))$ $(l=0, 1, \ldots, n-1)$ симметрическую группу S_{3n+1}?

11. Каждое подмножество из S_n, состоящее больше чем из $n!/2$ перестановок порождает S_n. Доказать это.

12. Доказать, что все циклы длины 3 вместе с какой-нибудь транспозицией являются системой образующих симметрической группы S_n.

§ 8. ПОДГРУППЫ СИММЕТРИЧЕСКИХ ГРУПП. ГРУППЫ ПЕРЕСТАНОВОК

Некоторые множества перестановок из симметрической группы S_n сами могут образовывать группу относительно умножения перестановок.

Определение. Подмножество T множества S_n называется *подгруппой группы* S_n, если оно образует группу относительно операции умножения перестановок.

В частности, само множество S_n также является своей подгруппой, которую называют несобственной. С другой стороны, множество E_n, состоящее из одной тождественной перестановки ε, также является подгруппой группы S_n, как это следует из равенства

$$\varepsilon \circ \varepsilon = \varepsilon, \quad \varepsilon^{-1} = \varepsilon.$$

Подгруппа E_n называется *тривиальной* подгруппой симметрической группы S_n. Все подгруппы из S_n, отличные от S_n, называются *собственными подгруппами*. Следовательно, для собственной нетривиальной подгруппы G из S_n выполнено неравенство

$$1 < |G| < n!$$

Для любой подгруппы из S_n выполняются требования а) — г) из определения группы. Однако, проверяя будет ли данное подмножество из S_n подгруппой, нет необходимости устанавливать для него истинность всех свойств а) — г). Имеет место следующая

Теорема. *Непустое подмножество T симметрической группы S_n образует подгруппу тогда и только тогда, когда выполнены следующие условия*:

1) *произведение $\alpha \circ \beta$ любых двух перестановок α, β из T тоже содержится в T (T замкнуто относительно операции умножения перестановок)*;

2) *если $\alpha \in T$, то $\alpha^{-1} \in T$ (T замкнуто относительно перехода к обратной перестановке)*.

Доказательство. Согласно определению, произвольная подгруппа T группы S_n замкнута относительно операции умножения перестановок и относительно перехода к обратной перестановке. Тем самым, условие теоремы является необходимым. Покажем, что оно и достаточно. Пусть для некоторого непустого множества T перестановок из S_n выполнены условия теоремы 1) и 2). Условие 1) означает, что для множества T выполнено первое требование определения группы. Операция умножения перестановок из T ассоциативна, поскольку умножение произвольных перестановок, а следовательно, и тех, которые принадлежат T, подчиняется ассоциативному закону. Итак, для множества T и операции умножения перестановок выполнено второе требование определения группы. Далее, поскольку $T \neq \varnothing$, то существует по крайней мере одна перестановка α, принадлежащая T. По условию 2) теоремы отсюда имеем, что обратная перестановка α^{-1} тоже принадлежит T. Следовательно, по условию 1) перестановка $\alpha \circ \alpha^{-1} = \varepsilon$ содержится в T, т. е. выполнено третье из требований определения группы. Наконец, условие 2) показывает, что каждый элемент из T имеет обратный, который также принадлежит T. Таким образом, T является подгруппой симметрической группы S_n.

◀ Примеры. 1. Пусть H — множество перестановок из симметрической группы S_4:

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Проверим, является ли H подгруппой группы S_4. Имеем $\alpha^{-1} = \alpha$, $\beta^{-1} = \beta$, $\gamma^{-1} = \gamma$, следовательно, для множества H выполняется условие 2) только что доказанной теоремы. Кроме того,

$$\alpha \circ \beta = \beta \circ \alpha = \gamma, \quad \alpha \circ \gamma = \gamma \circ \alpha = \beta, \quad \beta \circ \alpha = \gamma \circ \beta = \alpha,$$
$$\alpha \circ \alpha = \alpha^2 = \varepsilon, \quad \beta \circ \beta = \beta^2 = \varepsilon, \quad \gamma \circ \gamma = \gamma^2 = \varepsilon$$

(проверьте!). Следовательно, произведение каждых двух элементов множества H является элементом того же множества, т. е. для H выполняется и условие 1) упомянутой теоремы. Из записанных нами равенств вытекает, что группа H абелева.

2. Пусть G — множество перестановок

$$\varepsilon=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix},\quad \alpha=\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix},\quad \beta=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix},$$
$$\gamma=\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix},\quad \delta=\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}.$$

Тогда $\alpha^{-1}=\delta$, $\beta^{-1}=\gamma$, $\delta^{-1}=\alpha$, $\gamma^{-1}=\beta$; следовательно, выполняется условие 2) теоремы о подгруппах группы S_n. Кроме того, выполняются равенства

$$\alpha\circ\beta=\beta\circ\alpha=\gamma,\quad \beta\circ\gamma=\gamma\circ\beta=\varepsilon,\quad \alpha^2=\beta,\quad \delta^2=\gamma,$$
$$\alpha\circ\gamma=\gamma\circ\alpha=\delta,\quad \beta\circ\delta=\delta\circ\beta=\alpha,\quad \beta^2=\delta,\quad \gamma^2=\alpha,$$
$$\alpha\circ\delta=\delta\circ\alpha=\varepsilon,\quad \gamma\circ\delta=\delta\circ\gamma=\beta$$

(проверьте!). Как видим, произведение каждых двух элементов множества G является элементом из G, следовательно, выполняется и условие 1). Поэтому множество G является подгруппой группы S_5, причем из приведенных равенств вытекает, что группа G абелева.

3. Пусть T — множество перестановок

$$\alpha=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\quad \varepsilon=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},$$
$$\beta=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\quad \gamma=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}.$$

Это множество не является подгруппой группы S_4, так как для него не выполняется ни одно из условий 1), 2). Действительно,

$$\gamma^{-1}=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\notin T,\qquad \alpha\circ\gamma=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\notin T. ▶$$

Симметрическая группа S_n имеет много разных подгрупп, причем их число очень быстро возрастает с увеличением числа n.

Ряд примеров мы приведем в следующем параграфе. Полностью описать все подгруппы группы S_n удается лишь для небольших n, а для n больших изучаются лишь общие свойства таких подгрупп.

Задача. Описать все подгруппы симметрической группы S_3.

Решение. 1) Опишем сначала подгруппы, которые состоят из двух элементов. Если H — такая подгруппа, то в нее входит элемент ε и еще какой-то другой элемент α. Элемент, обратный к α, не может совпадать с ε, поэтому $\alpha^{-1}=\alpha$. Последнее равенство можно записать так: $\alpha^2=\varepsilon$. Следовательно, α — перестановка второго порядка, т. е. цикл длины 2. Таким образом, существует не больше трех подгрупп второго порядка группы S_3. Это такие подмножества множества S_3:

$$A=\{\varepsilon, (1, 2)\}, \quad B=\{\varepsilon, (2, 3)\}, \quad C=\{\varepsilon, (1, 3)\}.$$

Теперь, пользуясь сформулированной выше теоремой, легко убедиться, что подмножества A, B, C действительно являются подгруппами, так как для каждого из них выполняются условия 1), 2) этой теоремы.

2) Опишем подгруппы, которые состоят из трех элементов. Если $G=\{\varepsilon, \alpha, \beta\}$ — такая подгруппа, то элементы α, β должны иметь порядок 3. Действительно, если один из них, например α, имеет порядок 2, то $\alpha^{-1}=\alpha$, и, поскольку каждый элемент имеет лишь один обратный, отсюда получаем, что и $\beta^{-1}=\beta$, т. е. $\beta^2=\varepsilon$. Но легко проверить непосредственно, что произведением любых двух элементов φ, ψ, $\varphi\neq\psi$, второго порядка является элемент, который имеет порядок 3. Следовательно, при таких предположениях произведение $\alpha\circ\beta$ не принадлежит G и G не есть подгруппа.

Рассмотрим теперь случай, когда перестановки α и β имеют порядок 3, т. е. $G=\{\varepsilon, (1, 2, 3), (1, 3, 2)\}$. Имеем $\alpha^{-1}=\beta$, $\beta^{-1}=\alpha$, $\alpha\circ\beta=\beta\circ\alpha=\varepsilon$, $\alpha^2=\beta$, $\beta^2=\alpha$, т. е. подмножество G множества S_3 действительно является подгруппой группы S_5. Легко убедиться непосредственно, что подмножества множества S_3, состоящие из 4 или 5 элементов, подгрупп не образуют. Это непосредственно следует также из теоремы Лагранжа, которая будет рассмотрена в § 11.

Итак, симметрическая группа S_3 содержит шесть подгрупп, учитывая саму группу S_3 как свою несобственную подгруппу и тривиальную подгруппу E_3.

При решении многих задач подгруппы симметрической группы S_n появляются и исследуются независимо, т. е. тот факт, что они являются подгруппами S_n, существенной роли не играет — сама объемлющая группа в рассмотрениях не участвует. В таких ситуациях подгруппы симметрической группы S_n называются просто *группами перестановок* на множестве $\{1, 2, \ldots, n\}$. Группы перестановок

принято обозначать парами символов, одним из которых обозначается сама группа, а другим — множество, на котором действуют перестановки из этой группы. Для наиболее употребительных групп перестановок употребляются стандартные обозначения, некоторые из которых будут приведены ниже.

◀ Примеры. 4. Пусть $M=\{1, 2, 3, 4\}$, K — множество перестановок

$$\varepsilon=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix},\quad \alpha=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix},$$

$$\beta=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix},\quad \gamma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}.$$

Множество K образует группу относительно операции умножения перестановок. (Проверьте!) Поэтому можно говорить о группе перестановок (K, M). Она называется *четверной группой Клейна.*

5. Пусть $M=\{1, 2, \ldots, n\}$. Рассмотрим множество перестановок, состоящее из всевозможных степеней цикла $\alpha=(1, 2, \ldots, n)$. Согласно утверждениям § 6 в последовательности

$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1},\ \alpha^n=\varepsilon$$

все перестановки будут различными. Убедимся, что множество перестановок

$$C_n=\{\varepsilon,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1}\}$$

образует группу относительно умножения перестановок. В самом деле, произведение перестановок α^i, α^j $(1\leqslant i, j\leqslant n)$ определяется равенством

$$\alpha^i\circ\alpha^j=\begin{cases}\alpha^{i+j}, & \text{если } i+j<n,\\ \alpha^{i+j-n}, & \text{если } i+j\geqslant n.\end{cases}$$

Следовательно, при любых i, j $(1\leqslant i, j\leqslant n)$ произведение $\alpha^i\circ\alpha^j$ принадлежит C_n. Обратной к перестановке α^i будет перестановка α^{n-i}, поскольку $\alpha^i\circ\alpha^{n-i}=\alpha^{i+(n-i)}=\alpha^n=\varepsilon$. Таким образом, для множества C_n выполняются условия теоремы о подгруппах S_n, т. е. оно образует группу относительно умножения подстановок. Группа перестановок (C_n, M) называется *циклической группой на n символах* и обозначается C_n.

6. Обобщим пример 5. Пусть $\alpha\neq\varepsilon$ — произвольная перестановка из S_n, имеющая порядок k. Тогда перестановки $\alpha, \alpha^2, \ldots, \alpha^k=\varepsilon$ все различные, и множество $\{\varepsilon, \alpha, \alpha^2, \ldots$

..., $\alpha^{k-1}\}$ образует группу относительно операции умножения перестановок. Эта группа называется циклической группой, порожденной перестановкой α, и обозначается $\langle\alpha\rangle$. Можно говорить и о циклических подгруппах симметрической группы S_n. Циклической будет, например, подгруппа из примера 2; каждая подгруппа группы S_3 также циклическая. Однако подгруппа из примера 1 циклической не является. ▶

Упражнения

1. Доказать следующее усиление теоремы о подгруппах S_n, позволяющее сокращать проверки:

Подмножество T симметрической группы S_n образует подгруппу тогда и только тогда, когда оно замкнуто относительно умножения, т. е. произведение любых двух элементов из T снова принадлежит T.

2. Описать все подгруппы S_4, состоящие из трех перестановок. Сколько их?

3. Сколько подгрупп второго порядка содержит группа S_5.

4. Подгруппа любой группы перестановок определяется так же, как и подгруппа S_n. Описать все подгруппы:

а) четверной группы Клейна; б) циклической группы C_4; в) циклической группы C_5.

5. Пусть $M=\{1, 2, \ldots, n\}$. *Стабилизатором элемента* $m \in M$ называется множество всех перестановок α из S_n, таких, что $(m)\alpha=m$. Доказать, что стабилизатор любого элемента из M является подгруппой.

6. Пусть $M=\{1, 2, \ldots, n\}$, $A \subset M$. Стабилизатором подмножества A называется множество St_A всевозможных перестановок α из S_n, таких, что для произвольного элемента $a \in A$ и перестановки $\alpha \in St_A$ имеем $(a)\alpha \in A$. Доказать, что стабилизатор любого подмножества из M образует подгруппу.

7. Говорят, что перестановки $\alpha, \beta \in S_n$ коммутируют, если $\alpha \circ \beta = \beta \circ \alpha$. Множество всевозможных элементов произвольной группы, которые коммутируют с каждым ее элементом, называется центром группы. Доказать, что центр любой группы перестановок является ее подгруппой.

8. Найти центр группы S_4. Каков центр циклических групп C_n $(n \geqslant 2)$?

9. Каких порядков могут быть циклические подгруппы в симметрической группе S_6?

10. Каков наивысший порядок циклических подгрупп симметрической группы S_{11}?

§ 9. ГРУППЫ СИММЕТРИЙ

Одним из наиболее употребляемых примеров групп и, в частности, групп перестановок, являются группы, которыми «измеряется» симметричность геометрических фигур как плоских, так и пространственных. В этом параграфе мы приведем соответствующие примеры.

Рассмотрим сначала **симметрию плоских фигур**. Плоская фигура может иметь *ось симметрии* (одну или несколько) — прямую, которая разбивает ее на две части (рис. 21), каждая из которых является зеркальным отражением другой. В этом случае фигура называется *симметричной относительно прямой*.

Другим типом симметрии является *симметрия относительно точки* (рис. 22), которая называется *центром симметрии*, а фигура — *центральносимметричной*. Это понятие естественным образом обобщается. А именно: будем говорить, что точка O есть *центр симметрии n-го порядка* для фигуры M, если фигура M совмещается с собой при поворотах на углы, кратные $2\pi/n$. Например, на рис. 23 изображена фигура, имеющая центр симметрии порядка 3.

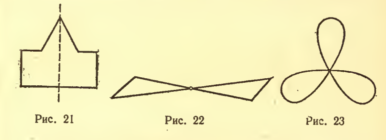


Рис. 21 Рис. 22 Рис. 23

Каждому типу симметрии соответствует преобразование симметрии — преобразование множества точек плоскости, определяемое этим типом. Так, если O — центр симметрии n-го порядка, то соответствующим преобразованием симметрии является преобразование вращения всех точек плоскости вокруг точки O на угол $2\pi/n$ (см. пример 8 § 2). Для определенности будем считать, что поворот осуществляется против движения часовой стрелки. А то, что некоторая фигура симметрична, означает, что она самосовмещается при соответствующем преобразовании симметрии. Таким образом, *обозрение всех симметрий фигуры равносильно обозрению всех преобразований плоскости, при которых она самосовмещается*. Понятно, что эти преобразования являются биекциями. Поэтому множество всех таких преобразований относительно умножения преобразований образует группу, которая является как бы мерой степени симметричности данной фигуры. Преобразования симметрии многих плоских фигур естественно описываются перестановками, т. е. их симметричность «измеряется» некоторыми группами перестановок.

Опишем эти группы в случае, когда рассматриваемая фигура является правильным многоугольником.

1. Группа симметрий правильного треугольника. Занумеруем вершины правильного треугольника числами 1, 2, 3 (рис. 24) и будем характеризовать каждое его самосовмещение φ перестановкой на множестве вершин треугольника

$$\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix},$$

где $i_k = (k)\varphi$ — номер места, которое после выполнения преобразования φ заняла вершина k, $k = 1, 2, 3$. Центр правильного треугольника O является центром симметрии порядка 3, т. е. повороты $\varphi_0 = \varepsilon$, φ_1, φ_2 на углы $0, 2\pi/3$,

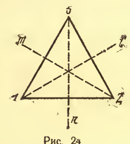


Рис. 24

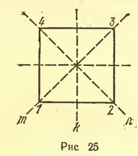


Рис 25

$4\pi/3$ соответственно вокруг точки O против часовой стрелки переводят треугольник в себя. Кроме того, имеется три осевых симметрии φ_3, φ_4, φ_5, определяемых осями симметрии l, m, n соответственно, проходящими через вершины правильного треугольника и середины его противоположных сторон (рис. 24). Принятое нами соответствие между самосовмещениями треугольника и перестановками множества вершин треугольника дает

$$\varphi_0 \sim \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \varphi_1 \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,\ 2,\ 3),$$

$$\varphi_2 \sim \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,\ 3,\ 2), \qquad \varphi_3 \sim \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,\ 3),$$

$$\varphi_4 \sim \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,\ 3), \qquad \varphi_5 \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,\ 2).$$

Таким образом, группа симметрий правильного треугольника — это симметрическая группа S_3.

2. Группа симметрий квадрата. Все самосовмещения квадрата являются либо вращениями $\alpha_0 = \varepsilon$, α_1, α_2, α_3 на углы 0, $\pi/2$, π, $3\pi/2$ соответственно вокруг центра квадрата, либо симметриями α_4, α_5, α_6, α_7 относительно осей

k, l, m, n соответственно, проходящих через середины противоположных сторон и через противоположные вершины (рис. 25). Соответствие между самосовмещениями квадрата и перестановками на множестве вершин квадрата при принятой на рис. 25 нумерации вершин квадрата имеет вид

$$\alpha_1 \sim (1,\ 2,\ 3,\ 4),\quad \alpha_2 \sim (1,\ 3)\circ(2,\ 4),\quad \alpha_3 \sim (1,\ 4,\ 3,\ 2),$$
$$\alpha_4 \sim (1,\ 2)\circ(3,\ 4),\ \alpha_5 \sim (1,\ 4)\circ(2,\ 3),\ \alpha_6 \sim (2,\ 4),\ \alpha_7 \sim (1,\ 3).$$

Таким образом, группа симметрий квадрата является собственной подгруппой симметрической группы S_4. Она обозначается символом D_4.

3. Группа симметрий правильного n-угольника состоит из n вращений на углы $0,\ 2\pi/n,\ 4\pi/n,\ \ldots,\ 2(n-1)\pi/n$ вокруг центра n-угольника и n симметрий относительно прямых. Положение осей симметрии зависит от четности числа n. При n четном имеется $n/2$ осей симметрии, проходящих через середины противолежащих сторон и $n/2$ осей, проходящих через противолежащие вершины (и центр) многоугольника. При n нечетном осями симметрии являются прямые, проходящие через вершины (и центр) n-угольника и середины противолежащих сторон. Таким образом, группа симметрий правильного n-угольника состоит из $2n$ преобразований. Если эти преобразования описывать перестановками множества вершин правильного n-угольника, то соответствующая группа перестановок является подгруппой симметрической группы S_n. Эта группа перестановок называется *группой диэдра* и обозначается D_n.

4. Группа симметрий многоугольника, изображенного на рис. 26, состоит из тождественного преобразования $\alpha_0 = \varepsilon$, симметрий α_1 и α_2 относительно осей l и m соответственно и центральной симметрии α_3 с центром O. Они описываются такими перестановками множества $\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$:

$$\alpha_1 \sim (1,\ 2)\circ(3,\ 6)\circ(4,\ 5),\quad \alpha_2 \sim (1,\ 5)\circ(2,\ 4),$$
$$\alpha_3 \sim (1,\ 4)\circ(2,\ 5)\circ(3,\ 6).$$

Для пространственных тел можно говорить о следующих типах симметрии:

а) *зеркальная симметрия* (симметрия относительно плоскости);

б) *осевая симметрия* (симметрия относительно прямой);

в) *центральная симметрия* (симметрия относительно точки).

По аналогии с плоским случаем понятие осевой симметрии естественно обобщается. Прямая называется *осью симметрии n-го порядка*, если тело совмещается с собой при вращениях вокруг прямой на углы, кратные $2\pi/n$. Каждому типу симметрии соответствует свое преобразование пространства, и *симметричность тела* означает, что оно самосовмещается при соответствующем преобразовании пространства. Множество всех тех преобразований, при которых тело совмещается с собой, образует *группу симметрии данного тела*. Симметрию многогранников и некоторых других тел можно характеризовать перестановками множества их вершин. В этом случае группа симметрии также является некоторой группой перестановок. Приведем несколько примеров такого описания.

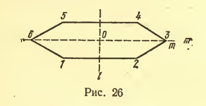


Рис. 26

Рис. 27

5. **Группа симметрий тетраэдра.** Тетраэдр (рис. 27) имеет 4 оси симметрии l_1, l_2, l_3, l_4 3-го порядка, проходящие через его вершины 1, 2, 3, 4 и центры противолежащих граней. Вокруг каждой оси, кроме тождественного, возможны еще два вращения. Им соответствуют такие перестановки:

$$\text{вокруг оси } l_1 \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

$$\text{вокруг оси } l_2 \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

$$\text{вокруг оси } l_3 \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix},$$

$$\text{вокруг оси } l_4 \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

Кроме того, имеется 3 оси симметрии 2-го порядка, проходящие через середины A, B, C, D, E, F скрещивающихся ребер. Поэтому имеется еще 3 (по числу пар скрещивающихся ребер) нетождественных преобразования,

которым соответствуют перестановки:

$$\text{вокруг оси } AB \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\text{вокруг оси } CD \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

$$\text{вокруг оси } EF \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Итак, вместе с тождественным преобразованием получаем 12 перестановок. При указанных преобразованиях тетраэдр самосовмещается, поворачиваясь в пространстве; его точки при этом не изменяют своего положения относительно друг друга. Совокупность выписанных 12 перестановок замкнута относительно умножения, поскольку последовательное выполнение вращений тетраэдра снова будет вращением. Таким образом, получаем группу, которая называется *группой вращений тетраэдра*.

При других преобразованиях пространства, являющихся самосовмещениями тетраэдра, внутренние точки тетраэдра передвигаются относительно друг друга. А именно: тетраэдр имеет 6 плоскостей симметрии, каждая из которых проходит через одно из его ребер и середину противолежащего ребра. Симметриям относительно этих плоскостей отвечают следующие транспозиции на множестве вершин тетраэдра:

Плоскость	Транспозиция
ребро (2, 3), точка A	(1, 4)
ребро (2, 4), точка C	(1, 3)
ребро (1, 2), точка E	(3, 4)
ребро (1, 4), точка B	(2, 3)
ребро (1, 3), точка D	(2, 4)
ребро (3, 4), точка F	(1, 2)

Уже на основании этих данных можно утверждать, что группа всевозможных симметрий тетраэдра состоит из 24 преобразований. В самом деле, каждая симметрия, самосовмещая тетраэдр в целом, должна как-то переставлять его вершины, ребра и грани. В частности, как уже было сказано, в данном случае симметрии можно характеризовать перестановками вершин тетраэдра. Поскольку тетраэдр имеет 4 вершины, его группа симметрий не может состоять больше чем из 24 преобразований. Иными словами, она либо совпадает с симметрической группой S_4, либо является ее подгруппой. Выписанные выше симметрии тетраэдра относительно плоскостей определяют все-

возможные транспозиции на множестве его вершин. Поскольку эти транспозиции порождают симметрическую группу S_4, получаем требуемое. Таким образом, любая перестановка вершин тетраэдра определяется некоторой его симметрией. Однако этого нельзя сказать о произвольной перестановке ребер тетраэдра. Если условиться обозначать каждое ребро тетраэдра той же буквой, что и его середину, то, скажем, перестановки на множестве ребер

$$\begin{pmatrix} A & B & C & D & E & F \\ F & E & A & B & D & C \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D & E & F \\ C & D & F & E & B & A \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F \\ A & B & D & C & F & E \end{pmatrix}$$

отвечают соответственно двум вращениям вокруг оси l_1 и вращению вокруг оси AB. Выписав перестановки на множестве $\{A, B, C, D, E, F\}$ для всех преобразований симметрии, получим некоторую подгруппу симметрической группы S_6, состоящую из 24 перестановок. Группа перестановок вершин тетраэдра и группа перестановок его ребер — разные группы перестановок, поскольку они действуют на разных множествах. Но за ними «видна» одна и та же группа — группа преобразований пространства, оставляющих тетраэдр на месте! В следующем параграфе для описания такой ситуации мы введем специальное понятие — *изоморфизм групп*, а о группах, «похожих» друг на друга в указанном смысле, будем говорить, что они *изоморфны*.

6. Группа симметрий куба. Симметрии куба, как и симметрии тетраэдра делятся на два типа — самосовмещения, при которых точки куба не изменяют своего положения относительно друг друга, и преобразования, оставляющие куб в целом на месте, но передвигающие его точки относительно друг друга. Преобразования первого типа мы, как и в случае тетраэдра, будем называть *вращениями*. Все вращения, очевидно, образуют группу, которая называется *группой вращений куба*. Опишем сначала строение этой группы.

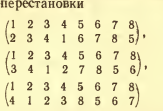
Имеется ровно 24 вращения куба вокруг различных осей симметрии.

В самом деле, при поворотах куба место нижней грани может занять любая из 6 граней куба (рис. 28). Для каждой из 6 возможностей — когда указано, какая именно грань расположена внизу, — имеется 4 различных расположения куба, соответствующих его поворотам вокруг

оси, проходящей через центры верхней и нижней граней, на углы 0, $\pi/2$, π, $3\pi/2$. Таким образом, получаем $6\cdot 4 = 24$ вращений куба. Укажем их в явном виде.

Куб имеет центр симметрии (точка пересечения его диагоналей), 3 оси симметрии четвертого порядка, 4 оси симметрии третьего порядка и 6 осей симметрии второго порядка. Достаточно рассмотреть вращения вокруг осей симметрии.

а) Оси симметрии четвертого порядка — это оси O_1O_2, O_3O_4, O_5O_6, проходящие через центры противоположных граней. Вокруг каждой из этих осей имеется по три нетождественных вращения, а именно вращения на углы $\pi/2$, π, $3\pi/2$. Этим вращениям соответствуют 9 перестановок вершин куба, при которых вершины противоположных граней переставляются циклически и согласовано. Например, перестановки



$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&1&6&7&8&5\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&4&1&2&7&8&5&6\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4&5&6&7&8\\4&1&2&3&8&5&6&7\end{pmatrix}$$

Рис. 28

отвечают поворотам вокруг оси O_1O_2.

б) Осями симметрии третьего порядка являются диагонали куба. Вокруг каждой из четырех диагоналей [1, 7], [2, 8], [3, 5], [4, 6] имеется по два нетождественных вращения на углы $2\pi/3$, $4\pi/3$. Например, вращения вокруг диагонали [1, 7] определяют такие перестановки вершин куба:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\1&5&6&2&8&3&7&3\end{pmatrix}, \quad \begin{pmatrix}1&2&3&4&5&6&7&8\\1&4&8&5&2&3&7&6\end{pmatrix}.$$

Всего получаем 8 таких вращений.

в) Осями симметрии второго порядка будут прямые, соединяющие середины противолежащих ребер куба. Имеется шесть пар противоположных ребер (например, [1, 2], [7, 8]), каждая пара определяет одну ось симметрии, т. е. получаем 6 осей симметрии второго порядка. Вокруг каждой из этих осей имеется одно нетождественное вращение. Всего — 6 вращений. Вместе с тождественным преобразованием получаем $9+8+6+1=24$ различных вращения. Итак, все вращения куба указаны. Вращения куба определяют перестановки на множествах его вершин, ребер,

граней и диагоналей. Рассмотрим, как действует группа вращений куба на множестве его диагоналей. Различные вращения куба переставляют диагонали куба по-разному, т. е. им соответствуют различные перестановки на множестве диагоналей (проверьте!). Поэтому группа вращений куба определяет группу перестановок на множестве диагоналей, состоящую из 24 перестановок. Поскольку куб имеет лишь 4 диагонали, группа всех таких перестановок совпадает с симметрической группой на множестве диагоналей. Итак, любая перестановка диагоналей куба соответствует некоторому его вращению, причем разным перестановкам соответствуют разные вращения.

Опишем теперь всю группу симметрий куба. Куб имеет три плоскости симметрии, проходящие через его центр. Симметрии относительно этих плоскостей в сочетании со всеми вращениями куба дают нам еще 24 преобразования, являющихся самосовмещениями куба. Поэтому полная группа симметрий куба состоит из 48 преобразований.

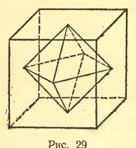


Рис. 29

7. Группа симметрий октаэдра. Октаэдр — один из пяти правильных многогранников (кроме тетраэдра и куба, к ним относятся еще икосаэдр и додекаэдр). Его можно получить, соединяя центры граней куба и рассматривая тело, ограниченное плоскостями, которые определяются соединительными прямыми для соседних граней (рис. 29). Поэтому любая симметрия куба одновременно является симметрией октаэдра и наоборот. Таким образом, группа симметрий октаэдра такая же, как и группа симметрий куба, и состоит из 48 преобразований.

В каждом из рассмотренных в пп. 5—7 примеров имеет место следующая закономерность. Группа симметрий правильного многогранника состоит из $2l$ преобразований, где l — число его плоских углов. Это утверждение имеет место для всех правильных многогранников, его можно доказать в общем виде, не находя всех симметрий многогранников, как это было нами сделано.

Упражнения

1. Доказать, что для всех $n \geqslant 2$ группа диэдра D_n неабелева.

2. Определить типы и порядки всех перестановок из групп диэдра D_7 и D_8.

3. *Системой образующих группы перестановок* G называется такое множество T ее элементов, что любую перестановку из G можно разложить в произведение перестановок из T. Система образующих T *неприводима*, если из нее нельзя выбросить ни одной перестановки так, чтобы оставшееся множество было системой образующих группы G. Проверьте, что вращение правильного n-угольника на угол $2\pi/n$ и любая из симметрий относительно прямых, сохраняющих n-угольник, являются неприводимой системой образующих группы его симметрий. Существует ли неприводимая система образующих группы D_n, состоящая из элементов порядка 2? Существуют ли неприводимые системы образующих D_n, состоящие из разного количества перестановок?

4. Описать группу симметрий звезды, изображенной на рис. 30. Каков порядок этой группы?

5. Отличаются ли группы симметрий фигур, изображенных на рис. 31?

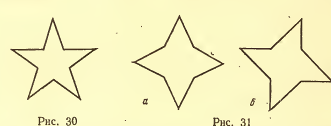


Рис. 30 Рис. 31

6. Определить типы всех перестановок из группы симметрий тетраэдра, действующей на множестве его ребер.

7. Тетраэдр можно вписать в куб так, что ребра тетраэдра будут диагоналями граней куба. При этом любое вращение куба определяет некоторое вращение тетраэдра. Какие вращения куба определяют одинаковые вращения тетраэдра? Сколько их для каждого вращения тетраэдра?

8. Найти центр группы вращений тетраэдра.

9. Каков наивысший порядок циклических подгрупп, содержащихся в группе вращений куба? в группе всех его симметрий?

10. Описать группу всех симметрий прямой призмы, в основе которой лежит правильный n-угольник. Выделить в ней подгруппу вращений. Совпадают ли эти группы?

§ 10. ТЕОРЕМА КЭЛИ

Из рассмотренных в предыдущих параграфах примеров видно, что симметрические группы весьма богаты подгруппами. Более того, *любую конечную группу можно рассматривать как подгруппу подходящим образом выбранной симметрической группы.* Это утверждение было установлено в середине прошлого столетия английским математиком А. Кэли и теперь называется его именем. Прежде чем точно сформулировать теорему Кэли, введем понятие

изоморфизма групп — одного из основных понятий теории групп.

Изучать группы можно по-разному. Один из возможных и, по существу, главный подход состоит в том, что при изучении группы исследуются свойства групповой операции независимо от природы элементов группы. При других подходах к исследованию свойств групп опираются на определенные факты, касающиеся природы элементов группы. С точки зрения первого подхода может оказаться, что в группах с элементами различной природы групповая операция с точностью до обозначений одна и та же. Поясним сказанное на примере.

Пусть K — группа перестановок с групповой операцией умножением перестановок

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$

введенная в § 8 в примере 4 (четверная группа Клейна), L — группа из упражнения 2 б) к § 4, т. е. группа функций

$$y=x,\quad y=-x,\quad y=1/x,\quad y=-1/x,$$

определенных на множестве действительных чисел без 0 с групповой операцией суперпозицией функций. Это совершенно разные группы, поскольку они состоят из разных объектов: в первом случае — перестановки, а во втором — функции действительного аргумента. Введем теперь согласованные обозначения для элементов этих групп следующим образом:

Обозначение	Элемент из K	Элемент из L
e	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$	$y=x$
a	$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$	$y=-x$
b	$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$	$y=1/x$
c	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$	$y=-1/x$

Согласно этой таблице, скажем, перестановка $\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$ и функция $y=-x$ обозначены одним и тем же

символом a. Если теперь составить таблицы умножения для групп K и L в новых обозначениях их элементов, то получим как в первом, так и во втором случае следующую таблицу (проверьте!):

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Итак, элементы групп K и L можно «переназвать» так, что в «новых наименованиях» таблицы умножения этих групп будут совпадать. Но таблица умножения полностью определяет групповую операцию. Таким образом, из сказанного видно, что если не обращать внимания на природу элементов групп K и L, то групповые операции в этих группах можно не различать. Неразличимые в таком смысле группы принято называть изоморфными. Сформулируем теперь общее определение изоморфизма групп.

Определение. Группы G_1 и G_2 называются *изоморфными*, если между их элементами можно установить взаимно однозначное соответствие, называемое *изоморфизмом* и обозначаемое стрелкой $\leftrightarrow$, которое сохраняет групповую операцию, т. е. такое, что для произвольных элементов $g_1, g_1' \in G_1$ из условий $g_1 \leftrightarrow g_2$, $g_1' \leftrightarrow g_2'$ следует, что $g_1 * g_1' \leftrightarrow g_2 * g_2'$.

Если группы G_1 и G_2 изоморфны, а элементы из G_1 и соответствующие им элементы из G_2 одинаково обозначить, то понятно, что таблицы умножения этих групп в таких обозначениях будут совпадать. Очевидно, что имеет место и обратное: если элементы групп G_1, G_2 можно так обозначить, что в этих обозначениях их таблицы умножения совпадают, то группы G_1 и G_2 изоморфны.

Отношение изоморфизма групп имеет следующие свойства:

1) *Нейтральному элементу e_1 группы G_1 соответствует нейтральный элемент e_2 группы G_2.*

Действительно, пусть элементу $e_1 \in G_1$ при изоморфизме $G_1 \leftrightarrow G_2$ соответствует некоторый элемент a из G_2. Тогда элементу $e_1^2 = e_1 * e_1$ соответствует, согласно основному свойству изоморфизма, элемент $a * a = a^2$. Однако $e_1^2 = e_1$. Поскольку изоморфизм — взаимно однозначное соответствие, отсюда

получаем, что $a^2 = a$. Умножая правую и левую части этого равенства на элемент a^{-1} (например, слева), получим $a^{-1} * a^2 = a^{-1} * a$, т. е. $a = e_2$.

2) *Для произвольного элемента* $g_1 \in G_1$ *соответствие* $g_1 \leftrightarrow g_2$ *влечет за собой* $g_1^{-1} \leftrightarrow g_2^{-1}$.

В самом деле, пусть элементу g_1^{-1} соответствует при изоморфизме некоторый элемент $h \in G_2$. Тогда произведению $g_1 * g_1^{-1}$ будет соответствовать произведение $g_2 * h$. Но $g_1 * g_1^{-1} = e_1$, и по первому свойству изоморфизма отсюда получаем, что $g_2 * h = e_2$. Следовательно, $h = g_2^{-1}$.

3) Понятно, что *любая группа изоморфна сама себе и отношение изоморфизма симметрично* (если группа G_1 изоморфна группе G_2, то и наоборот — группа G_2 изоморфна группе G_1).

4) *Изоморфные группы состоят из одинакового числа элементов.*

Изоморфизм между данными двумя группами не обязательно определяется единственным образом. Например, легко проверяется, что любое взаимно однозначное соответствие между элементами рассматриваемых выше групп K и L, при котором нейтральные элементы этих групп соответствуют друг другу, будет изоморфизмом. Существует 6 взаимно однозначных соответствий между подмножествами элементов групп K и L, отличных от нейтральных, т. е. изоморфизм между группами K и L можно установить шестью различными способами.

Теперь мы можем строго сформулировать и доказать основное утверждение этого параграфа.

Теорема Кэли. *Любая конечная группа изоморфна некоторой группе перестановок на множестве своих элементов.*

Доказательство. Пусть $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$, g — некоторый элемент из этой группы, т. е. $g = g_i$ для какого-то i $(0 \leqslant i \leqslant n-1)$. По элементу g определим преобразование $\hat{g}$ множества G, задавая его таблицей значений

$$\hat{g} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-1} \\ g_0 * g & g_1 * g & g_2 * g & \cdots & g_{n-1} * g \end{pmatrix}.$$

Поскольку множество G замкнуто относительно умножения, все элементы вида $g_i * g$ $(0 \leqslant i \leqslant n-1)$ принадлежат G, т. е. эта таблица действительно определяет преобразование над множеством G. Более того, все элементы ряда

$$g_0 * g, \quad g_1 * g, \quad g_2 * g, \quad \ldots, \quad g_{n-1} * g$$

различны, поскольку из равенства $g_i * g = g_j * g$ получаем, умножая его правую и левую части справа на элемент g^{-1},

$$(g_i * g)\, g^{-1} = (g_j * g) * g^{-1} \quad \text{или} \quad g_i * (g * g^{-1}) = g_j * (g * g^{-1}).$$

Поскольку $g * g^{-1} = e$, то $g_i = g_j$, т. е. $i = j$. Таким образом, преобразование $\hat{g}$ является перестановкой множества G.

Пусть $R(G)$ — множество всех перестановок вида $\hat{g}$, построенных по элементам группы G. Установим соответствие между элементами группы G и перестановками из $R(G)$ по правилу

$$g \leftrightarrow \hat{g} = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-1} \\ g_0 * g & g_1 * g & g_2 * g & \dots & g_{n-1} * g \end{pmatrix}.$$

Понятно, что различным элементам из G соответствуют различные перестановки из $R(G)$, поскольку они по-разному действуют на нейтральный элемент группы G. Итак, это соответствие взаимно однозначное. Проверим, что оно сохраняет групповую операцию, т. е. для любых элементов g, g' из G выполняется условие $g * g' \leftrightarrow \hat{g} \cdot \widehat{g'}$. Иными словами, это означает, что для любых элементов g, g' из G имеет место равенство $\widehat{g * g'} = \hat{g} \cdot \widehat{g'}$. Перестановка $\widehat{g * g'}$ согласно определению задается таблицей

$$\begin{pmatrix} g_0 & g_1 & \dots & g_{n-1} \\ g_0 * (g * g') & g_1 * (g * g') & \dots & g_{n-1} * (g * g') \end{pmatrix},$$

т. е. под ее действием произвольный элемент $g_i \in G$ переходит в элемент $g_i * (g * g')$. Произведение перестановок $\hat{g}$, $\widehat{g'}$ на любой элемент $g_i \in G$ действует так:

$$g_i \xrightarrow{\hat{g}} g_i * g \xrightarrow{\widehat{g'}} (g_i * g)\, g'.$$
$$\underbrace{\qquad\qquad\qquad}_{\hat{g} \cdot \widehat{g'}}$$

В силу ассоциативности умножения в группе G получаем, что для любого $i = 0, 1, \dots, n-1$ выполняется равенство

$$g_i * (g * g') = (g_i * g) * g', \text{ т. е. } (g_i)\,\widehat{g * g'} = (g_i)\,(\hat{g} \cdot \widehat{g'}).$$

А это и означает, что для перестановок $\hat{g}$, $\widehat{g'}$ на множестве G выполнено равенство $g * \widehat{g'} = \hat{g} \cdot \widehat{g'}$. Теорема доказана.

Отметим, что при доказательстве мы не проверяли отдельно замкнутость множества $R(G)$ относительно умножения перестановок — это автоматически следует из того, что $R(G)$ — изоморфный образ группы G. Группу подста-

новок $R(G)$ принято называть *правым регулярным представлением группы* G. Аналогично можно строить *левое регулярное представление*, при котором произвольному элементу g из G взаимно однозначно соответствует перестановка

$$\check{g} = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-1} \\ g*g_0 & g*g_1 & g*g_2 & \dots & g*g_{n-1} \end{pmatrix}$$

(g умножается последовательно слева на все элементы группы G). Левое регулярное представление группы G ей не изоморфно, поскольку произведению $g \cdot g'$ элементов из G соответствует перестановка $\check{g}' \cdot \check{g}$, т. е. множители переставляются. Такие группы называются *антиизоморфными*.

Упражнения

1. Доказать, что из условий $|G_1| = |G_2| = 2$ или $|G_1| = |G_2| = 3$ следует, что группы G_1 и G_2 — изоморфны.

2. Любая группа, состоящая из четырех элементов, изоморфна либо четверной группе Клейна либо циклической группе четвертого порядка. Доказать это.

3. Доказать, что группа подстановок на множестве $\{1, 2, 3, 4, 5, 6\}$, состоящая из подстановок

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix},$$

изоморфна симметрической группе S_3.

4. Группа перестановок (G, M) называется регулярной, если для произвольных двух элементов m_1, m_2 из множества M существует в точности одна перестановка α из группы G, такая, что $(m_1)\alpha = m_2$. Чему равен стабилизатор произвольного элемента из M (см. задачу 5 из § 8) в группе G?

5. Проверить, что правое регулярное представление произвольной группы является регулярной группой перестановок.

6. Построить правое регулярное представление следующих групп:

а) группы симметрий правильного треугольника;

б) группы функций $y = x$, $y = -x$, $y = 1/x$, $y = -1/x$, определенных на множестве действительных чисел кроме нуля.

7. Если группы G_1 и G_2 изоморфны и группы G_2 и G_3 тоже изоморфны, то изоморфными будут также группы G_1 и G_3. Доказать это.

§ 11. ТЕОРЕМА ЛАГРАНЖА

Пусть G и H — группы перестановок, причем $H \subset G$, т. е. как принято говорить, H является подгруппой группы G. Одной из первых теорем теории групп является

теорема, устанавливающая связь между порядками групп G и H, доказанная в несколько иных терминах Лагранжем еще в конце XVIII столетия. Эта простая по идее доказательства теорема очень часто применяется как в самой теории групп, так и во всех приложениях, одно из которых мы рассмотрим ниже.

Теорема Лагранжа. *Если H — подгруппа группы G, то ее порядок является делителем порядка G.*

Доказательство. Пусть ε, α_1, α_2, ..., α_{n-1} — все перестановки, содержащиеся в группе G, $\beta_0=\varepsilon$, β_1, ..., β_{m-1} — все перестановки из H (т. е. $m\leqslant n$). Если $H=G$, то утверждение теоремы справедливо, поэтому предположим, что $H\neq G$ (H — собственная подгруппа G). В силу этого предположения существует перестановка $\gamma_1\in G$, такая, что $\gamma_1\notin H$. Рассмотрим ряд перестановок

$$\beta_0\circ\gamma_1=\gamma_1,\ \beta_1\circ\gamma_1,\ \ldots,\ \beta_{m-1}\circ\gamma_1. \qquad (1)$$

Все перестановки этого ряда различны: если бы для каких-то i, j имело место равенство $\beta_i\circ\gamma_1=\beta_j\circ\gamma_1$, то, умножив его правую и левую части на γ_1^{-1}, мы получили бы равенство $\beta_i=\beta_j$. Кроме того, ни одна из них не содержится в подгруппе H: если бы для какого-то номера i имело место включение $\beta_i\circ\gamma_1\in H$, то это означало бы, что $\beta_i\circ\gamma_1=\beta_j$ для какого-то j. Из этого равенства имеем $\gamma_1=\beta_i^{-1}\circ\beta_j$, а так как H — группа перестановок, то $\gamma_1\in H$, что противоречит выбору этой перестановки.

Если перестановками группы H и ряда (1) исчерпаны все перестановки из G, то $|G|=2|H|$, и все доказано. В противном случае найдется такая перестановка $\gamma_2\in G$, что $\gamma_2\notin H$ и γ_2 не содержится в ряде (1). Определим для нее ряд перестановок

$$\beta_0\circ\gamma_2=\gamma_2,\quad \beta_1\circ\gamma_2,\quad \ldots,\quad \beta_{m-1}\circ\gamma_2. \qquad (2)$$

Аналогично проверяется, что а) все перестановки ряда (2) различны; б) они не содержатся в H; в) ни одна из них не встречается среди перестановок ряда (1).

Если перестановками из подгруппы H и рядов (1) и (2) исчерпываются все элементы группы G, то $|G|=3|H|$ и все доказано. В противном случае продолжаем процесс выбора перестановок γ_i и построения рядов вида (1) и (2) дальше. Так как группа G конечная, то на каком-то, например на k-м, шаге все перестановки из G будут исчерпаны. Иными словами, все их можно расположить таким

образом:

$$\begin{array}{lllll} \beta_0 & \beta_1 & \beta_2 & \dots & \beta_{m-1}, \\ \beta_0\circ\gamma_1 & \beta_1\circ\gamma_1 & \beta_2\circ\gamma_1 & \dots & \beta_{m-1}\circ\gamma_1, \\ \beta_0\circ\gamma_2 & \beta_1\circ\gamma_2 & \beta_2\circ\gamma_2 & \dots & \beta_{m-1}\circ\gamma_2, \\ \dots & \dots & \dots & \dots & \dots \\ \beta_0\circ\gamma_{k-1} & \beta_1\circ\gamma_{k-1} & \beta_2\circ\gamma_{k-1} & \dots & \beta_{m-1}\circ\gamma_{k-1}, \end{array} \quad (3)$$

при этом все перестановки в каждой из строк различны и любые 2 строки не имеют общих элементов. Поскольку общее число элементов в (3) равно n (порядок группы G), а число элементов в каждой строке равно m (порядок группы H), то имеем равенство $n=mk$, т. е. m является делителем n, и теорема доказана.

Число k называют *индексом подгруппы H в группе G* и обозначают $[G:H]$. Из доказательства теоремы Лагранжа мы получаем, что имеет место равенство

$$|G|=|H|[G:H].$$

Так как порядок циклической подгруппы, порожденной перестановкой $\alpha\in G$, совпадает с порядком перестановки α, то из теоремы Лагранжа получаем, что *порядок любой перестановки из G — делитель $|G|$*.

Теорема Лагранжа позволяет также существенно упростить решение задачи описания всех подруп данной группы. Например, *если порядок группы G есть простое число, то в G нет нетривиальных собственных подгрупп* (согласно теореме Лагранжа).

Собственные подгруппы из S_3 могут состоять из двух и трех перестановок (делители числа $3!=6$), поэтому непосредственную проверку, о которой идет речь в задаче из § 8, можно опустить. А ведь эта проверка длинная, так как есть $C_6^4+C_6^5=21$ подмножество из S_3, состоящее из 4 или 5 элементов. Даже на этих двух примерах видно, насколько существенным может быть применение теоремы Лагранжа.

Упражнения

1. Множества перестановок, стоящие в рядах таблицы (3), называются *правыми* (так как γ_i умножается справа) *классами смежности*, а таблицу (3) естественно назвать *таблицей разложения группы G на правые классы смежности по подгруппе H*. Вполне аналогично можно построить таблицу разложения группы G на *левые* классы смежности по подгруппе H. Постройте таблицы разложения группы S_3 на классы смежности как правые, так и левые по подгруппе $A=\{\varepsilon, (1, 2)\}$; по подгруппе $B=\{\varepsilon, (1, 2, 3), (1, 3, 2)\}$.

2. Доказать, что вращения правильного шестиугольника вокруг центра на углы, кратные $\pi/3$, образуют подгруппу в группе всех его симметрий. Составить таблицы разложения на правые и левые классы смежности группы симметрий шестиугольника по подгруппе всех вращений. Обобщить это на случай произвольного n-угольника.

3. Если H — подгруппа индекса 2 в группе G, то правые и левые классы смежности по этой подгруппе совпадают. Докажите.

4. Пусть $k_1, k_2, \ldots, k_n$ — решение (k_i — натуральные) уравнения

$$x_1+x_2+\ldots+x_n=m$$

(m — произвольное натуральное). Тогда $k_1! \cdot k_2! \cdot \ldots \cdot k_n!$ является делителем $m!$ Докажите.

5. Выпишите все числа, которые, согласно теореме Лагранжа, могут быть порядками элементов в группе D_{12}. Существуют ли в группе D_{12} перестановки таких порядков?

6. Тот же вопрос для группы S_4.

§ 12. ОРБИТЫ ГРУППЫ ПЕРЕСТАНОВОК. ЛЕММА БЕРНСАЙДА

Рассматривая группы перестановок, мы ограничивались изучением их действия на элементы некоторого множества. Но ведь если такое действие определено, то перестановки поэлементно «передвигают» и подмножества данного множества. При изучении свойств действий на подмножествах первым шагом является, естественно, описание тех подмножеств, которые данная группа перестановок в целом не передвигает. В связи с этим возникает понятие орбиты группы перестановок на данном множестве.

Пусть G — группа перестановок на множестве $M=\{1, 2, \ldots, n\}$. Подмножество $O \subset M$ называется *орбитой группы* G, если

а) $(a)\alpha \in O$ для любого $\alpha \in G$ и любого $a \in O$; т. е. действие перестановок из G на элементы O не выводит за пределы O;

б) любые два элемента из O можно перевести друг в друга некоторой перестановкой из G.

Всякая группа перестановок $G=\{\varepsilon=\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ *имеет орбиты.*

Для доказательства выберем произвольный элемент $a \in M$ и рассмотрим множество $O(a)=\{a=(a)\alpha_0, (a)\alpha_1, \ldots, (a)\alpha_{k-1}\}$. Оно будет орбитой группы G, так как

а) если $\alpha_i \in G$ и $b=(a)\alpha_j \in O(a)$, то $(b)\alpha_i=(a)(\alpha_j \cdot \alpha_i) \in O(a)$, так как $\alpha_j \cdot \alpha_i \in G$ (ведь G — группа);

б) если $b=(a)\alpha_i$ и $c=(a)\alpha_j$ — произвольные элементы из $O(a)$, то $b=(a)\alpha_i=(a)(\varepsilon \cdot \alpha_i)=(a)(\alpha_j \cdot \alpha_j^{-1} \cdot \alpha_i)=(c)\alpha_j^{-1} \cdot \alpha_i$; и при этом $\alpha_j^{-1} \cdot \alpha_i \in G$, так как G — группа.

Оказывается, что *орбитами подобного вида исчерпываются все типы орбит*. Более точно, если O — орбита группы G и $a \in O$, то $O = O(a)$. Справедливость этого утверждения вытекает непосредственно из определения орбиты группы.

Ясно, что любые две орбиты $O(a)$ и $O(b)$ либо совпадают (если $b \in O(a)$), либо не пересекаются (если $b \notin O(a)$). Отсюда (почти так же как и при доказательстве теоремы Лагранжа) следует, что *множество M распадается в объединение непересекающихся подмножеств — орбит группы G*. В частности, может случиться, что единственной орбитой группы G будет само множество M, как это имеет место для групп D_n (проверьте!). Группы с таким свойством называются *транзитивными*. Таким образом, группа перестановок G на множестве M транзитивна, если любой элемент $a \in M$ может быть получен из любого другого элемента $b \in M$ под действием подходящим способом выбранной перестановки $\alpha \in G$: $a = (b)\alpha$. Все другие группы перестановок называются *интранзитивными*.

В связи с разбиением множества M на орбиты группы перестановок G возникают следующие два вопроса:

1) Сколько орбит имеет группа G на множестве M?

2) Какова длина каждой из этих орбит, т. е. из скольких элементов они состоят?

Сформулируем вначале утверждение, позволяющее выяснить ответ на второй вопрос. Оно формулируется с использованием понятия стабилизатора элемента из M. А именно: для любого элемента $a \in M$ можно рассмотреть множество G_a всех перестановок из G, для которых точка a является неподвижной. Это множество, очевидно, является группой (еще один способ образования групп перестановок!), которая и называется стабилизатором точки a.

Теорема. *Длина орбиты $O(a)$ равна индексу стабилизатора G_a в группе G, т. е.*

$$|O(a)| = |G| : |G_a|.$$

Доказательство. Пусть $G = \{\alpha_0 = \varepsilon, \alpha_1, \ldots, \alpha_{k-1}\}$, $G_a = \{\beta_0 = \varepsilon, \beta_1, \ldots, \beta_{s-1}\}$. Для подсчета различных элементов в последовательности a, $(a)\alpha_1, \ldots, (a)\alpha_{k-1}$ удобно особым образом расположить в ряд элементы группы G. Для этого вспомним примененное при доказательстве теоремы Лагранжа разложение группы G в правые классы смежности по подгруппе G_a. Существуют перестановки $\gamma_0 = \varepsilon, \gamma_1, \ldots, \gamma_{l-1}$ из группы G, такие, что все переста-

новки ряда.

$$\alpha_0=\beta_0\circ\gamma_0=\varepsilon,\quad \alpha_1=\beta_1\circ\gamma_0,\quad \ldots,\quad \alpha_{s-1}=\beta_{s-1}\circ\gamma_0,$$
$$\alpha_s=\beta_0\circ\gamma_1,\quad \alpha_{s+1}=\beta_1\circ\gamma_1,\quad \ldots,\quad \alpha_{2s-1}=\beta_{s-1}\circ\gamma_1,\qquad (1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_{(l-1)s}=\beta_0\circ\gamma_{l-1},\quad \alpha_{(l-1)s+1}=\beta_1\circ\gamma_{l-1},\quad \ldots,\quad \alpha_{ls-1}=\beta_{s-1}\circ\gamma_{l-1}$$

попарно различны и исчерпывают всю группу G. Для любого $i=0, \ldots, l-1$ примененне s перестановок α_{is}, $\alpha_{is+1}, \ldots, \alpha_{(i+1)s-1}$, образующих i-ю строку таблицы (1), к элементу a дает один н тот же элемент $(a)\gamma_i$. Все l элементов $(a)\gamma_i$ попарно различны. Действительно, если бы $(a)\gamma_i=(a)\gamma_j$ для некоторых i, j, то $a=(a)\gamma_j\circ\gamma_i^{-1}$, т. е. перестановка $\gamma_j\circ\gamma_i^{-1}\in G_a$. Но это возможно только тогда, когда γ_i н γ_j содержатся в одном правом классе смежности группы G по подгруппе G_a, чего быть не может.

Таким образом, длина орбиты $O(a)$ равна l, т. е. числу строк в таблице (1). А это число в § 10 и было названо индексом подгруппы в группе.

Проиллюстрируем понятие орбиты группы и доказанную теорему на примере 4 из § 9, где рассматривалась группа перестановок $G=\{\varepsilon, \alpha, \beta, \gamma\}$, действующая на множестве $M=\{1, 2, 3, 4, 5, 6\}$. Имеем $(1)\varepsilon=1$, $(1)\alpha=5$, $(1)\beta=2$, $(1)\gamma=4$, т. е. $O(1)=\{1, 2, 4, 5\}$. Выбирая какой-нибудь элемент из M, не принадлежащий $O(1)$, скажем 6, получим $(6)\varepsilon=6$, $(6)\alpha=6$, $(6)\beta=3$, $(6)\gamma=3$, т. е. $O(6)=\{3, 6\}$. Таким образом, группа перестановок G на множестве M имеет две орбиты:

$$O(1)=\{1, 2, 4, 5\},\quad O(6)=\{3, 6\},$$

и поэтому является ннтранзитивной.

Стабилизатор G_1 точки 1 нз $O(1)$ состонт нз одной перестановкн ε. Поэтому $[G:G_1]=4=|O(1)|$. Стабилизатор G_6 точки 6 нз $O(6)$ состонт из перестановок ε и α. Разложение группы G на правые классы смежности по подгруппе $G_6=\{\varepsilon, \alpha\}$ имеет вид

$$\varepsilon,\quad \alpha,\quad \varepsilon\circ\beta=\beta,\quad \alpha\circ\beta=\gamma.$$

Поэтому $[G:G_6]=2=|O(6)|$.

Докажем теперь утверждение, чисто историческн называемое леммой Бернсайда по нмени английского математика-алгебраиста В. Бернсайда (1852—1927), который, по-вндимому, первым опубликовал его доказательство в своей книге по теорни конечных групп (1911 г.). Это простое утверждение является основой теории перечисления, разработанной Д. Пойа и рядом других математи-

ков, — теории, находящей широкие применения в кибернетике, технике, органической химии, биологии и т. д.

Пусть $\chi(a)$ — число неподвижных точек перестановки α, $t(G)$ — число орбит группы перестановок $G=\{\alpha_0=\varepsilon, \alpha_1, \ldots, \alpha_{k-1}\}$, действующей на множестве $M=\{1, 2, \ldots, n\}$.

Лемма Бернсайда. *Для любой группы перестановок имеет место равенство*

$$t(G)=\frac{1}{|G|}\sum_{\alpha\in G}\chi(\alpha).$$

Доказательство. Рассмотрим отношение «перестановка α сохраняет неподвижным элемент m» между перестановками группы G и элементами множества M. Сопоставим парам (α, m), $\alpha\in G$, $m\in M$, вершины прямоугольной сети и отметим те из них, для которых соответствующая пара (α, m) находится в указанном отношении, т. е. $(m)\alpha=m$ (рис. 32). Иными словами, построим график указанного отношения. Число отмеченных точек (точек, принадлежащих графику) можно подсчитать двумя способами: определить число отмеченных точек на каждой вертикали и просуммировать полученные величины или же определить число таких точек по каждой горизонтали и затем вычислить их сумму.

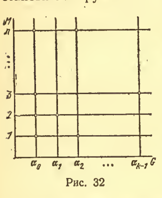


Рис. 32

Согласно определению отношения на каждой вертикали отмечаются все точки, сохраняемые перестановкой α, соответствующей этой вертикали. Их число равно $\chi(\alpha)$. Поэтому число всех точек графика равно

$$\chi(\alpha_0)+\chi(\alpha_1)+\ldots+\chi(\alpha_{k-1})=\sum_{\alpha\in G}\chi(a).$$

С другой стороны, на каждой горизонтали отмечаются все перестановки, сохраняющие элемент $m\in M$, отвечающий этой горизонтали. Мы знаем, что они образуют группу G_m — стабилизатор элемента m — и их число, согласно предыдущей теореме, равно

$$|G_m|=|G|:|O(m)|.$$

Поэтому при втором способе подсчета числа отмеченных точек графика рассматриваемого отношения получаем выражение

$$|G_1|+|G_2|+\ldots+|G_n| = \sum_{m\in M} |G_m|. \qquad (2)$$

Однако если элементы $i, j \in M$ содержатся в одной орбите, то $O(i)=O(j)$ и поэтому $|G_i|=|G|:|O(i)|=|G|:|O(j)|=|G_j|$. Пусть $O_1, O_2, \ldots, O_t$ — все орбиты группы G, такие, что $M=O_1\cup O_2\cup\ldots\cup O_t$, и слагаемые в этом объединении не пересекаются. Разобьем сумму (2) на части так, чтобы внутри каждой из частей суммирование шло по элементам некоторой орбиты:

$$\sum_{m\in M}|G_m| = \sum_{m\in O_1}|G_m| + \sum_{m\in O_2}|G_m| + \ldots + \sum_{m\in O_t}|G_m|.$$

Каждое из t слагаемых в правой части этого равенства можно преобразовать следующим образом:

$$\sum_{m\in O}|G_m| = \sum_{m\in O}\frac{|G|}{|O(m)|} = \frac{|G|}{|O|}\sum_{m\in O}1 = \frac{|G|}{|O|}|O| = |G|.$$

Поэтому

$$\sum_{m\in M}|G_m| = \underbrace{|G|+\ldots+|G|}_{t} = t|G|.$$

Таким образом, при втором способе подсчета мы получили $t|G|$ отмеченных точек графика. Приравнивая величины, полученные при первом и втором способах, получим

$$t|G| = \sum_{\alpha\in G}\chi(\alpha),$$

т. е. $t=t(G)=\frac{1}{|G|}\sum_{\alpha\in G}\chi(\alpha)$. Лемма доказана.

В частности, если группа G транзитивная, т. е. $t(G)=1$, то по лемме Бернсайда

$$|G| = \sum_{\alpha\in G}\chi(\alpha).$$

Упражнения

1. Пусть G — группа симметрий куба. Найдите порядок стабилизатора некоторой вершины в этой группе. Какие перестановки в нем содержатся?

2. Проверьте правильность утверждения леммы Бернсайда на примере группы G (пример 4 § 9).

3. Перестановкн α н β нз группы G сопряжены в ней, если в G найдется такая перестановка γ, что $\gamma^{-1}\circ\alpha\circ\gamma=\beta$. Доказать, что а) каждая перестановка сопряжена сама с собой; б) если перестановка α сопряжена с перестановкой β, то н, наоборот, перестановка β сопряжена с перестановкой α; в) еслн α сопряжена с β, а β — с γ, то α сопряжена с γ.

4. Из свойств а), б), в) упражнення 3 следует, что множество G разбнвается в объедннение непересекающнхся подмножеств перестановок, попарно сопряженных между собой, которые называются классами сопряженных перестановок группы G. Докажнте это.

5. Если перестановки α н β сопряжены, то $\chi(\alpha)=\chi(\beta)$, т. е. функцня χ постоянна на классах сопряженных элементов G.

6. Используя предыдущую задачу, показать, что формулу для определення чнсла орбит группы G можно перепнсать в виде

$$t(G)=\frac{1}{|G|}\sum_{i=1}^{s}\chi_i\psi_i,$$

где χ_i — общее значенне $\chi(\alpha)$ для перестановок i-го класса сопряженных перестановок, ψ_i — чнсло перестановок в i-м классе сопряженных перестановок, s — чнсло классов сопряженных перестановок.

7. Доказать, что сопряженные перестановки имеют однннаковый тип.

8. Еслн перестановкн α н β сопряжены, то при любом $n\in Z$ перестановки α^n н β^n тоже будут сопряженнымн. Доказать это.

Следует ли нз сопряженностн пар перестановок α_1, α_2 н β_1, β_2 сопряженность нх произведений?

9. Группа вращенни куба естественным образом определяет группу перестановок на множестве его ребер. Определнть тнпы всех перестановок нз этой группы.

10. Каждое вращенне куба естественным образом переставляет его гранн, т. е. группа вращенни куба определяет группу перестановок на множестве его граней. Доказать, что эта группа транзнтнвна. Определнть стабнлизатор одной из точек (граней куба) в этой группе.

§ 13. КОМБИНАТОРНЫЕ ЗАДАЧИ

Рассмотрим два простых примера, иллюстрирующих возможности применения леммы Бернсайда при решении комбинаторных задач на перечисление. Ряд примеров читатель найдет также в упражнениях к этому параграфу.

1. Раскраска вершин куба. Сколькими способами можно раскрасить вершины куба в три цвета (например, красный, синий и зеленый)?

На первый взгляд может показаться, что задача совсем простая. Поскольку каждую из восьми вершин куба можно раскрасить тремя способами, причем независимо от того, как раскрашены другие вершины, то множество всех вершин куба можно раскрасить $3^8=6561$ различными способами. Однако при таком подходе к решению задачи

молчаливо предполагается, что мы умеем различать вершины куба перед окраской, т. е., скажем, куб жестко закреплен или его вершины занумерованы. При этом полученный ответ можно интерпретировать следующим образом: можно так раскрасить 3^8 абсолютно одинаковых, жестко закрепленных кубов, что все они будут различаться. Для 3^8+1 кубов этого сделать уже нельзя.

Ситуация существенно меняется, если мы откажемся от предположения о том, что кубы жестко закреплены, так как по-разному окрашенные кубы можно повернуть так, что в новом положении их окраски совпадут (рис. 33).

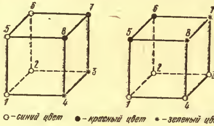


Рис. 33

Естественно считать, что два куба раскрашены одинаково, если их раскраски совпадают после некоторого вращения одного из кубов в пространстве. Будем говорить, что такие раскраски кубов *геометрически неотличимы*. Поэтому естественным уточнением задачи о раскраске является следующая задача:

Сколькими геометрически различными способами можно раскрасить вершины куба в три цвета.

Переформулируем теперь эту задачу так, чтобы стала понятной ее связь с леммой Бернсайда. Пусть M — множество всевозможных по-разному раскрашенных кубов одного размера, положение которых в пространстве фиксировано, $|M|=3^8$, G — группа всех вращений куба, состоящая из 24 перестановок. Группа G естественным образом определяет группу перестановок на множестве M. Именно: если $\alpha \in G$ — некоторое вращение, то каждому кубу из M можно сопоставить некоторый, вообще говоря, другой куб, который получается из первого при вращении α. Это соответствие является, очевидно, перестановкой на множестве M, которую будем обозначать $\tilde{\alpha}$. Группу всех таких перестановок множества M, определяемых перестановками из G, мы будем обозначать $\tilde{G}$. Ясно, что $|\tilde{G}|=|G|$.

То, что два куба K_1 и K_2 из M раскрашены геометрически одинаково, означает, что один из них можно перевести вращением в такое положение, в котором они неразличимы. Иными словами, существует такая перестановка $\tilde{\alpha} \in \tilde{G}$, что $(K_1)\tilde{\alpha} = K_2$, т. е. K_1 и K_2 содержатся в одной орбите группы $\tilde{G}$, действующей на множестве M. Таким образом, для того чтобы определить число геометрически различимых способов раскраски вершин куба, нужно найти количество орбит группы $\tilde{G}$ на множестве M.

Считая вершины кубов занумерованными числами 1, 2, 3, 4, 5, 6, 7, 8, раскраску каждого из 3^8 кубов можно однозначно охарактеризовать «словом» из 8 букв, каждая из которых есть либо *к*, либо *с*, либо *з*. То, что i-я буква слова равна *к* (или *с*, или *з*), означает, что i-я вершина при выбранной нумерации окрашена в красный цвет (или в синий, или в зеленый соответственно). Например, для кубов, изображенных на рис. 33, имеем соответственно последовательности *ссззсскк*, *ссссккзз*. Перестановки из группы $\tilde{G}$ переставляют такие последовательности. Например, если $\alpha = (1, 2, 3, 4) \circ (5, 6, 7, 8) \in G$, то перестановка $\tilde{\alpha}$ слово *сссссссз* переводит в *ссссзссс*, слово *ссззсскк* переводит в *сззсккс*, слова *сссссссс*, *кккккккк*, *зззззззз* оставляет неизменными и т. д. Выписать всю таблицу значений для перестановки $\tilde{\alpha}$ затруднительно, поскольку она состоит из 3^8 строк!

Для того чтобы применить лемму Бернсайда, необходимо определить число неподвижных точек каждой перестановки из $\tilde{G}$. Последовательность букв *к*, *с*, *з* будет неподвижной для перестановки $\tilde{\alpha} \in \tilde{G}$ тогда и только тогда, когда при разложении соответствующей перестановки $\alpha \in G$ в произведение циклов вершины куба, номера которых входят в один и тот же цикл, окрашены одним цветом. Например, если $\alpha = (1, 2, 3, 4) \circ (5, 6, 7, 8)$, то неподвижными относительно $\tilde{\alpha}$ будут слова, составленные целиком из одной буквы, и слова, составленные из двух разных букв, причем одна из них стоит на первых четырех местах в слове, а вторая — из четырех последующих. Поэтому имеется 9 неподвижных точек перестановки $\tilde{\alpha}$ на множестве M. Уже на этом примере видно, что подсчет числа неподвижных точек перестановок из $\tilde{G}$ сильно упрощается, если известны разложения в произведение циклов соответствующих перестановок из G. Если перестановка $\alpha \in G$ разложена в произведение k-циклов, то число ее непо-

движных точек равно 3^k ($1 \leqslant k \leqslant 8$). Поэтому сначала мы опишем разложения в произведение циклов для всех перестановок из группы G вращений куба.

а) Вокруг каждой из трех осей, соединяющих центры противоположных граней, имеется три нетождественных вращения. Им соответствуют перестановки

$$(1, 5, 8, 4) \circ (2, 6, 7, 3),$$
$$(1, 4, 3, 2) \circ (5, 8, 7, 6),$$
$$(1, 8) \circ (2, 7) \circ (3, 6) \circ (4, 5),$$
$$(1, 3) \circ (2, 4) \circ (5, 6) \circ (6, 8),$$
$$(1, 4, 8, 5) \circ (2, 3, 7, 6);$$
$$(1, 2, 3, 4) \circ (5, 6, 7, 8);$$
$$(1, 5, 6, 2) \circ (3, 4, 8, 7),$$
$$(1, 6) \circ (2, 5) \circ (3, 8) \circ (4, 7),$$
$$(1, 2, 6, 5) \circ (3, 7, 8, 4).$$

б) Вокруг каждой из четырех диагоналей, т. е. осей, соединяющих противоположные вершины куба, имеется по два нетривиальных вращения. Им соответствуют перестановки

$$(1) \circ (2, 5, 4) \circ (3, 6, 8) \circ (7),$$
$$(2) \circ (1, 3, 6) \circ (4, 7, 5) \circ (8),$$
$$(3) \circ (1, 6, 8) \circ (2, 7, 4) \circ (5),$$
$$(4) \circ (1, 3, 8) \circ (2, 7, 5) \circ (6),$$
$$(1) \circ (2, 4, 5) \circ (3, 8, 6) \circ (7),$$
$$(2) \circ (1, 6, 3) \circ (4, 5, 7) \circ (8),$$
$$(3) \circ (1, 8, 6) \circ (2, 4, 7) \circ (5),$$
$$(4) \circ (1, 8, 3) \circ (2, 5, 7) \circ (6).$$

в) Вокруг каждой из шести осей, соединяющих середины противоположных ребер, имеется одно нетривиальное вращение. Им соответствуют перестановки

$$(1, 5) \circ (2, 8) \circ (3, 7) \circ (4, 6),$$
$$(1, 2) \circ (3, 5) \circ (4, 6) \circ (7, 8),$$
$$(1, 7) \circ (2, 3) \circ (4, 6) \circ (5, 8),$$
$$(1, 7) \circ (2, 6) \circ (3, 5) \circ (4, 8),$$
$$(1, 7) \circ (2, 8) \circ (3, 4) \circ (5, 6),$$
$$(1, 4) \circ (2, 8) \circ (3, 5) \circ (6, 7).$$

Вместе с тождественной получаем 24 перестановки. Итак, в группе G вращений куба имеется

1 перестановка типа $\langle 1, 1, 1, 1, 1, 1, 1, 1\rangle$,
6 перестановок типа $\langle 4, 4\rangle$,
9 перестановок типа $\langle 2, 2, 2, 2\rangle$,
8 перестановок типа $\langle 1, 1, 3, 3\rangle$.

Перестановка первого типа имеет 3^8 неподвижных точек, любая из перестановок второго типа — 3^2, третьего и четвертого типов — 3^4 неподвижных точек. Поэтому согласно лемме Бернсайда имеем

$$t(\tilde{G}) = \frac{1}{24}(3^8 + 6\cdot 3^2 + 9\cdot 3^4 + 8\cdot 3^4) = 333.$$

Таким образом, *число геометрически различимых способов раскраски вершин куба в три цвета равно* 333.

2. Составление ожерелий. *Сколько различных ожерелий из семи бусин можно составить из бусин двух цветов — красного и синего?*

Для того чтобы стала понятной аналогия этой задачи с предыдущей, переформулируем ее следующим равносильным образом:

Сколькими геометрически различными способами можно раскрасить вершины правильного семиугольника в два цвета?

Здесь два способа раскраски неотличимы, если один из них можно получить из другого, применяя к семиугольнику либо преобразования вращения, либо симметрии относительно осей, т. е. перестановки из группы диэдра D_7. Если вершины семиугольника пронумерованы, имеется $2^7 = 128$ различных вариантов их раскраски, так как каждую вершину независимо от других можно раскрасить двумя способами.

Снова будем описывать раскраски словами длины 7, составленными из букв $к$ (вершина окрашена в красный цвет) и $с$ (вершина окрашена в синий цвет). На множестве N всех таких слов действует группа $\tilde{D}_7$ перестановок, задаваемых перестановками из D_7. Например, если $\alpha = (1, 2, 3, 4, 5, 6, 7)$, то перестановка $\tilde{\alpha}$ последнюю букву каждого слова переставляет в его начало, а остальные буквы не изменяет. Для того чтобы определить число орбит группы $\tilde{D}_7$ на множестве N, необходимо найти типы перестановок из D_7. Эта задача гораздо проще аналогичного вопроса для группы G из примера 1. Группа D_7 состоит из 14 перестановок множества $\{1, 2, 3, 4, 5, 6, 7\}$,

которые распределены по возможным типам так:

1 перестановка имеет тип $\langle 1, 1, 1, 1, 1, 1, 1\rangle$,
6 перестановок имеют тип $\langle 7\rangle$,
7 перестановок имеют тип $\langle 1, 2, 2, 2\rangle$.

Слово неподвижно относительно перестановки $\tilde{\alpha} \in \tilde{D}_7$, тогда и только тогда, когда буквы, стоящие на местах с номерами из одного цикла в перестановке α, совпадают. Поэтому тождественная перестановка имеет 2^7 неподвижных точек на N, перестановки второго типа — по 2, а перестановки третьего типа — по 2^4. Применяя лемму Бернсайда, получаем

$$t(\tilde{D}_7) = \frac{1}{14}(2^7 + 6\cdot 2 + 7\cdot 2^4) = 18.$$

Итак, *из бусин двух цветов можно составить* 18 *семибусенных ожерелий*.

Упражнения

1. Грани куба можно раскрасить: а) все в белый цвет; б) все в черный цвет; в) часть в белый, а остальные в черный. Сколько имеется разных способов раскраски?

2. Сколько различных ожерелий можно составить из двух синих, двух белых и двух красных бусин?

3. Сколькими геометрически различными способами три абсолютно одинаковые мухи могут усесться в вершинах правильного пятиугольника?

4. Сколько существует различных ориентированных графов с тремя вершинами?

5. Сколько существует различных неориентированных графов с четырьмя вершинами?

6. Сколькими способами можно раскрасить вершины куба в два цвета так, чтобы вершин каждого цвета было поровну?

7. Сколькими различными способами можно грани куба раскрасить в четыре цвета?

§ 14. ДЕЙСТВИЕ ПЕРЕСТАНОВКИ НА МНОГОЧЛЕН

Напомним, что многочлен — это сумма каких-то одночленов. Если все одночлены многочлена f образованы из символов $x_1, x_2, \ldots, x_n$, то будем обозначать такой многочлен $f(x_1, x_2, \ldots, x_n)$ и говорить, что это многочлен с n переменными. Например,

$$f(x_1, x_2) = x_1^2 x_2 + 2x_1 x_2 + 5x_1$$

— многочлен с двумя переменными, а

$$g(x_1, x_2, x_3) = 2x_1^2x_2x_3^2 + 5x_1^2x_2 + 6x_3$$

— многочлен с тремя переменными.

Пусть $f(x_1, x_2, \ldots, x_n)$ — некоторый многочлен с n переменными, $M = \{1, 2, \ldots, n\}$ — множество индексов при переменных. Для произвольной перестановки $\sigma \in S_n$ определим действие σ на многочлен $f(x_1, x_2, \ldots, x_n)$, положив

$$(f(x_1, x_2, \ldots, x_n))^\sigma = f^\sigma(x_1, x_2, \ldots, x_n) = f(x_{(1)\sigma}, x_{(2)\sigma}, \ldots, x_{(n)\sigma}).$$

◀ Пример 1. а) Если $f(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4^2 + x_1^2x_2x_3x_4 + x_1 + x_2 + 1$, а

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

то

$$f^\sigma(x_1, x_2, x_3, x_4) = x_2x_3x_1x_4^2 + x_2^2x_3x_1x_4 + x_2 + x_3 + 1.$$

б) Для многочлена

$$g(x_1, x_2, x_3, x_4) = x_1^3x_2x_3x_4 + x_1x_2^3x_3x_4 + x_1x_2x_3^3x_4$$

и перестановки σ из предыдущего примера имеем

$$g^\sigma(x_1, x_2, x_3, x_4) = x_2^3x_3x_1x_4 + x_2x_3^3x_1x_4 + x_2x_3x_1^3x_4 = g(x_1, x_2, x_3, x_4). \blacktriangleright$$

Из этого примера видно, что многочлен $f^\sigma(x_1, x_2, \ldots, x_n)$ может отличаться от $f(x_1, x_2, \ldots, x_n)$, а может и совпадать с ним.

Если $f^\sigma(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)$, то говорят, что многочлен f не изменяется под действием перестановки σ, или, иначе, *инвариантен относительно действия* σ. Понятно, что каждый многочлен от n переменных инвариантен относительно действия тождественной перестановки:

$$f^\varepsilon(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n).$$

Поскольку операция умножения двух перестановок означает их последовательное выполнение, то для любых перестановок σ, τ и произвольного многочлена $f(x_1, x_2, \ldots, x_n)$ имеем

$$((f(x_1, x_2, \ldots, x_n))^\sigma)^\tau = f^{\sigma \circ \tau}(x_1, x_2, \ldots, x_n).$$

Отсюда вытекает, что когда многочлен $f(x_1, x_2, \ldots, x_n)$ не изменяется под действием перестановок σ и τ, то он будет инвариантен и относительно их произведения. Кроме того, каждый многочлен $f(x_1, x_2, \ldots, x_n)$, инвариантный

относительно перестановки σ, будет инвариантным и относительно перестановки σ^{-1}. Поэтому множество всех перестановок, которые не меняют заданный многочлен $f(x_1, x_2, \ldots, x_n)$, образует группу. Эта группа называется *группой инерции многочлена* $f(x_1, x_2, \ldots, x_n)$.

◀ Пример 2. Найдем группу инерции многочлена

$$A(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

Имеем

$$A^{(1,2)}(x_1, x_2, x_3) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -A(x_1, x_2, x_3),$$
$$A^{(2,3)}(x_1, x_2, x_3) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -A(x_1, x_2, x_3),$$
$$A^{(1,3)}(x_1, x_2, x_3) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = -A(x_1, x_2, x_3),$$
$$A^{(1,2,3)}(x_1, x_2, x_3) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = A(x_1, x_2, x_3),$$
$$A^{(1,2,3)}(x_1, x_2, x_3) = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = A(x_1, x_2, x_3).$$

Следовательно, группой инерции многочлена $A(x_1, x_2, x_3)$ является множество $\{\varepsilon, (1, 2, 3), (1, 3, 2)\}$. ▶

Из этого примера видно, что многочлен $A(x_1, x_2, x_3)$ *меняет знак под действием любой транспозиции*. Этот результат обобщается на многочлены такого вида с бо́льшим числом переменных.

Многочлен $A(x_1, x_2, x_3)$ является произведением разностей $x_i - x_j$ для $i < j$, $i, j = 1, 2, 3$; поэтому многочлен такого вида с n переменными будет такой:

$$A(x_1, x_2, \ldots, x_n) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\ldots(x_1 - x_n) \times$$
$$\times (x_2 - x_3)(x_2 - x_4)\ldots(x_2 - x_n) \times$$
$$\times (x_3 - x_4)\ldots(x_3 - x_n) \times$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\times (x_{n-1} - x_n).$$

Он содержит $(n-1) + (n-2) + \ldots + 1 = n(n-1)/2$ сомножителей. Пусть (i, j), $i < j$ — произвольная транспозиция. Она действует лишь на те сомножители $x_k - x_l$, $k < l$, в которых по меньшей мере один из индексов k, l совпадает с i или j. Под действием транспозиции (i, j) знак сомножителя $x_i - x_j$ меняется на противоположный:

$$(x_i - x_j)^{(i,j)} = x_j - x_i = -(x_i - x_j).$$

Для других сомножителей, которые изменяются под действием транспозиции (i, j), имеем

а) если i, $j < k$, то $x_i - x_k$ переходит в $x_j - x_k$ и наоборот, не меняя знака;

б) если i, $j > k$, то $x_k - x_i$ переходит в $x_k - x_j$ и наоборот, не меняя знака;

в) если $i<k<j$, то x_i-x_k переходит в $x_j-x_k=-(x_k-x_j)$, а x_k-x_j переходит в $x_k-x_i=-(x_i-x_k)$, т. е. произведение $(x_i-x_k)(x_k-x_j)$ под действием (i, j) не изменяет знака.

Следовательно, произведение всех сомножителей многочлена $A(x_1, x_2, \ldots, x_n)$, кроме x_i-x_j, под действием (i, j) не изменяет знака, а сомножитель x_i-x_j изменяет знак на противоположный. Поэтому произведение всех сомножителей — многочлен $A(x_1, x_2, \ldots, x_n)$ — также изменяет знак:

$$A^{(i,\, j)}(x_1, x_2, \ldots, x_n)=-A(x_1, x_2, \ldots, x_n).$$

Поскольку каждую перестановку можно разложить в произведение транспозиций, то под действием любой перестановки многочлен $A(x_1, x_2, \ldots, x_n)$ может лишь изменить знак. Именно поэтому этот многочлен называется *знакопеременным многочленом с n переменными.*

Пусть $f(x_1, x_2, \ldots, x_n)$ — некоторый многочлен. Действуя на него всевозможными перестановками из S_n, получим, вообще говоря, какой-то набор разных многочленов:

$$f_1(x_1, x_2, \ldots, x_n),\ f_2(x_1, x_2, \ldots, x_n),\ \ldots,\ f_s(x_1, x_2, \ldots, x_n).$$

Сам многочлен $f(x_1, x_2, \ldots, x_n)$ в этом ряду обязательно встретится, так как $f^e=f$. Многочлен

$$f_1(x_1, x_2, \ldots, x_n)+f_2(x_1, x_2, \ldots, x_n)+\ldots+f_s(x_1, x_2, \ldots, x_n)$$

будем называть орбитальным для $f(x_1, x_2, \ldots, x_n)$. Орбитальный многочлен, как легко понять, инвариантен относительно любой перестановки из S_n.

◀ Пример 3. а) Для одночлена x_1^k орбитальным многочленом с n переменными будет многочлен

$$s_k=x_1^k+x_2^k+\ldots+x_n^k.$$

Такие многочлены называются степенными суммами от n переменных. В частности, степенными суммами с двумя переменными будут многочлены

$$s_1=x_1+x_2,\quad s_2=x_1^2+x_2^2,\quad s_3=x_1^3+x_2^3.$$

б) Для одночлена $x_1^2x_2^3x_3$ орбитальным многочленом с тремя переменными будет многочлен

$$x_1^2x_2^3x_3+x_1^2x_2x_3^3+x_1^3x_2^2x_3+x_1x_2^3x_3^2+x_1^3x_2x_3^2+x_1x_2^2x_3^3. ▶$$

Орбитальный многочлен с n переменными для одночлена $x_1^{l_1}x_2^{l_2}\ldots x_s^{l_s}$ будем обозначать $o_n\left(x_1^{l_1}x_2^{l_2}\ldots x_s^{l_s}\right)$.

Например,

$$o_2(x_1x_2^2) = x_1x_2^2 + x_1^2x_2,$$

$$o_3(x_1x_2^2) = x_1x_2^2 + x_1x_3^2 + x_1^2x_2 + x_1^2x_3 + x_2x_3^2 + x_2^2x_3.$$

Легко убедиться, что для любого n многочлен $o_n(x_1^kx_2^l)$ выражается через степенные суммы. Проверим это для случая $n=3$. Имеем

$$s_ks_l = (x_1^k + x_2^k + x_3^k)(x_1^l + x_2^l + x_3^l) = x_1^{k+l} + x_2^{k+l} + x_3^{k+l} + x_1^kx_2^l + x_1^kx_3^l + x_1^lx_2^k + x_2^kx_3^l + x_1^lx_3^k + x_2^lx_3^k = s_{k+l} + o_3(x_1^kx_2^l).$$

Следовательно, $o_3(x_1^kx_2^l) = s_ks_l - s_{k+l}$.

Интересным является вопрос о нахождении количества слагаемых в орбитальных многочленах. Понятно, что количество одночленов в многочленах $o_n(x_1^{l_1}x_2^{l_2}\ldots x_s^{l_s})$ не может превышать $n!$ Максимальное количество одночленов будем иметь только тогда, когда все переменные будут входить в одночлен с разными степенями, а если показатели переменных в одночлене будут повторяться, то оно будет меньше.

Упражнения

1. Пусть $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, а f — один из многочленов:
а) $x_1x_2^2x_3x_4^2 + 2x_1^2x_2x_3x_4 + 3x_1x_2^3$;
б) $x_1^2x_2^2x_3x_4 + x_1^2 + x_3$;
в) $x_1^2 + x_2^2 + x_3 + x_4$.
Найти f^σ.

2. Найти группу инерции многочлена
$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3^2x_4 + 2x_1^2x_2x_3x_4 + 5x_1 + 3x_2 + 1.$$

3. Из какого числа перестановок состоит группа инерции многочлена $A(x_1, x_2, x_3, x_4)$?

4. Для произвольной группы перестановок существует многочлен, для которого эта группа является группой инерции. Доказать это.

5. Сколько одночленов содержит многочлен $o_4(x_1^2x_2x_3^2x_4)$. Записать этот многочлен.

6. Доказать, что многочлен $o_n(x^kx^l)$ выражается через степенные суммы для любого n.

7. Сколько одночленов содержит многочлен вида $o_n(x_1x_2\ldots x_l)$ для разных n, l?

§ 15. ЧЕТНЫЕ И НЕЧЕТНЫЕ ПЕРЕСТАНОВКИ. ЗНАКОПЕРЕМЕННАЯ ГРУППА

Разложение перестановок из S_n в произведение транспозиций, вообще говоря, **не однозначно**, например:

$$(1, 2, 3) = (1, 3)\cdot(2, 3) = (1, 2)\cdot(1, 3).$$

Все-таки определенную характеристику, которая остается одинаковой для каждого из таких разложений, указать можно. Такой характеристикой является четность числа сомножителей в разложении. Точнее, справедлива такая важная

Теорема. *Если $\alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_s$ и $\beta_1 \circ \beta_2 \circ \ldots \circ \beta_t$ — разложения перестановки в произведение транспозиций, то числа s и t имеют одинаковую четность.*

Доказательство. Пусть φ — некоторая перестановка на множестве $M = \{1, 2, \ldots, n\}$, $\alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_s$, $\beta_1 \circ \beta_2 \circ \ldots \circ \beta_t$ — разложения φ в произведение транспозиций. Подействуем перестановкой φ на знакопеременный многочлен $A(x_1, x_2, \ldots, x_n)$. Как было установлено в предыдущем параграфе, A и A^{φ} могут отличаться лишь знаком, причем если α транспозиция, то $A^{\alpha} = -A$. Рассмотрим две последовательности многочленов:

$$A,\ A^{\alpha_1} = F_1,\quad F_1^{\alpha_2} = F_2,\quad \ldots,\quad F_{s-1}^{\alpha_s} = F_s,$$

$$A,\ A^{\beta_1} = G_1,\quad G_1^{\beta_2} = G_2,\quad \ldots,\quad G_{t-1}^{\beta_t} = G_t.$$

В каждой из них два соседних выражения отличаются лишь знаком. А поэтому

$$F_s = (-1)^s A, \qquad G_t = (-1)^t A.$$

С другой стороны, $F_s = G_t = A^{\varphi}$. Следовательно, $(-1)^s A = (-1)^t A$, т. е. s и t — числа одинаковой четности.

Теперь можно дать такое определение.

Перестановка называется *четной*, если она раскладывается в произведение четного числа транспозиций. В противном случае перестановка называется *нечетной*.

Таким образом, четными будут те и только те перестановки, которые оставляют без изменения знакопеременный многочлен $A(x_1, x_2, \ldots, x_n)$. Обозначим через A_n множество четных перестановок из S_n, а через B_n — множество всех нечетных. По доказанной теореме каждая перестановка $\varphi \in S_n$ принадлежит одному из этих множеств, причем A_n и B_n не имеют общих элементов.

Покажем, что множества A_n и B_n состоят из одинакового количества перестановок, т. е.

$$|A_n| = |B_n|. \qquad (1)$$

Для этого построим взаимно однозначное отображение Ψ множества A_n на множество B_n. Зафиксируем некоторую транспозицию α и поставим в соответствие каждому

элементу $\omega \in A_n$ перестановку $\omega \cdot \alpha$:

$$\Psi: \omega \to \omega \cdot \alpha.$$

Перестановки ω и $\omega \cdot \alpha$ — разной четности, т. е. $\omega \cdot \alpha \in B_n$ и отображение Ψ определено правильно.

Убедимся в том, что отображение Ψ биективно. Если $\beta, \gamma \in A_n$ и $\beta \neq \gamma$, то и $\beta \cdot \alpha \neq \gamma \cdot \alpha$, потому что равенство $\beta \cdot \alpha = \gamma \cdot \alpha$ можно было сократить на α и получить, вопреки условию, что $\beta = \gamma$.

Для каждой перестановки $\beta \in B_n$ существует перестановка $\gamma \in A_n$, а именно $\gamma = \beta \cdot \alpha^{-1} = \beta \cdot \alpha$, такая, что $(\gamma)\Psi = \beta$. Следовательно, отображение Ψ является одновременно и инъекцией, и сюръекцией Отсюда вытекает справедливость равенства (1).

Каждая транспозиция — нечетная перестановка. Равенство (2) § 7 показывает, что цикл нечетной длины — перестановка четная. Четной будет также тождественная перестановка ε. Понятно, что произведение четных перестановок — перестановка четная, произведение двух нечетных перестановок — также четная, а произведение четной на нечетную (или наоборот) — нечетная.

Если перестановка φ разложена в произведение транспозиций

$$\varphi = \delta_1 \cdot \delta_2 \cdot \ldots \cdot \delta_{s-1} \cdot \delta_s,$$

то обратной к φ будет перестановка

$$\varphi^{-1} = \delta_s \cdot \delta_{s-1} \cdot \ldots \cdot \delta_2 \cdot \delta_1,$$

так как из равенства

$$(\delta_1 \cdot \delta_2 \cdot \delta_{s-1} \cdot \ldots \cdot \delta_s) \cdot (\delta_s^{-1} \cdot \delta_{s-1}^{-1} \cdot \ldots \cdot \delta_2^{-1} \cdot \delta_1^{-1}) = \varepsilon$$

вытекает, что $\varphi^{-1} = \delta_s^{-1} \cdot \delta_{s-1}^{-1} \cdot \ldots \cdot \delta_2^{-1} \cdot \delta_1^{-1}$, а для транспозиций $\delta_i^{-1} = \delta_i$.

Отсюда получаем, что множество A_n образует подгруппу группы S_n. Эта подгруппа называется *знакопеременной группой перестановок.* Она играет очень важную роль в теории групп перестановок и в ее применениях.

Заметим, что четность перестановки можно определить, не раскладывая ее в произведение транспозиций. Достаточно лишь разложить перестановку в произведение циклов и подсчитать количество циклов четной длины. Если найденное число будет четным, то перестановка четная, в противном случае — нечетная (см. упражнение 11).

Упражнения

1. Какую характерную особенность имеет граф четной перестановки?

2. Какой наивысший порядок могут иметь элементы группы A_5?

3. Составить таблицу умножения группы A_4.

4. Какая из описанных нами в § 8 подгрупп S_3 будет знакопеременной?

5. Найти центр группы A_n (см. упражнение 4 § 9).

6. Доказать, что A_n — максимальная подгруппа S_n, отличная от S_n, т. е. каждая подгруппа, которая содержит A_n, совпадает или с A_n, или с S_n.

7. Доказать, что каждую четную перестановку можно разложить в произведение циклов длины три.

8. Можно ли разложить каждую четную перестановку из S_n, где n нечетно, в произведение циклов

$$(1,\ 2,\ 3),\quad (1,\ 4,\ 5),\quad \ldots,\quad (1,\ n-1,\ n)?$$

9. Говорят, что пара чисел i, j образует инверсию, если $i > j$. Доказать, что перестановка

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

будет четной тогда и только тогда, когда количество инверсий, образованных элементами ее второго ряда, — число четное.

10. Сколько имеется перестановок из S_{10}, в которых элементы второго ряда образуют ровно 6 инверсий?

11. Пусть $\langle k_1, k_2, \ldots, k_s\rangle$ — тип перестановки $\varphi \in S_n$. Разность $n-s$ называется декрементом этой перестановки. Доказать, что четность перестановки совпадает с четностью ее декремента.

§ 16. СИММЕТРИЧЕСКИЕ И ЧЕТНОСИММЕТРИЧЕСКИЕ МНОГОЧЛЕНЫ

Многочлен $f(x_1, x_2, \ldots, x_n)$ называется *симметрическим*, если он является инвариантным относительно действия любой перестановки из S_n, т. е. *группой инерции такого многочлена является вся симметрическая группа* S_n.

Например, симметрическими будут такие многочлены с n переменными:

$$\sigma_1(x_1,\ x_2,\ \ldots,\ x_n) = x_1 + x_2 + \ldots + x_n,$$
$$\sigma_2(x_1,\ x_2,\ \ldots,\ x_n) = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,$$
$$\sigma_3(x_1,\ x_2,\ \ldots,\ x_n) = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_n(x_1,\ x_2,\ \ldots,\ x_n) = x_1x_2\ \ldots\ x_n.$$

Действительно, орбитальный многочлен любого одночлена — симметрический, а

$$\sigma_1(x_1, x_2, \ldots, x_n) = o_n(x_1), \quad \sigma_2(x_1, x_2, \ldots, x_n) = \\ = o_n(x_1x_2), \ldots, \sigma_n(x_1, x_2, \ldots, x_n) = o_n(x_1x_2 \ldots x_n).$$

Многочлены $\sigma_1, \sigma_2, \ldots, \sigma_n$ называются *элементарными симметрическими многочленами*. Запишем их полностью для $n=2$, $n=3$:

$$\sigma_1(x_1, x_2) = x_1 + x_2, \quad \sigma_1(x_1, x_2, x_3) = x_1 + x_2 + x_3,$$
$$\sigma_2(x_1, x_2) = x_1x_2, \quad \sigma_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3,$$
$$\sigma_3(x_1, x_2, x_3) = x_1x_2x_3.$$

Непосредственно видно, что а) сумма симметрических многочленов — симметрический многочлен; б) произведение симметрических многочленов — симметрический многочлен. Поэтому если в произвольный многочлен $g(y_1, y_2, \ldots, y_n)$ с n переменными подставить вместо $y_1, y_2, \ldots, y_n$ элементарные симметрические многочлены $\sigma_1, \sigma_2, \ldots, \sigma_n$, то получим некоторый многочлен от $x_1, x_2, \ldots, x_n$, который будет симметрическим. Например, если

$$g(y_1, y_2) = y_1^2y_2 + 5y_2 + 2,$$

то

$$g(\sigma_1, \sigma_2) = (x_1 + x_2)^2x_1x_2 + 5x_1x_2 + 2 = \\ = x_1^3x_2 + 2x_1^2x_2^2 + x_1x_2^3 + 5x_1x_2 + 2$$

— симметрический многочлен.

Оказывается, что так можно получить каждый симметрический многочлен.

Теорема. *Каждый симметрический многочлен является многочленом от элементарных симметрических многочленов.*

Эта теорема называется основной теоремой о симметрических многочленах. Мы докажем эту теорему лишь для многочленов с тремя неизвестными. Рассмотрение этого случая даст нам возможность обозреть все этапы полного доказательства.

Понятно, что каждый симметрический многочлен с произвольным числом переменных является суммой орбитальных многочленов. А потому для доказательства теоремы в случае $n=3$ достаточно убедиться, что многочлены вида $o_3(x_1^k)$, $o_3(x_1^kx_2^l)$, $o_3(x_1^kx_2^lx_3^m)$ можно представить в виде многочленов от $\sigma_1, \sigma_2, \sigma_3$.

1) Убедимся методом математической индукции по числу k, что каждая степенная сумма $s_k = x_1^k + x_2^k + x_3^k$

выражается через элементарные симметрические многочлены. Действительно, $s_1=x_1+x_2+x_3$ совпадает с σ_1, $s_2=x_1^2+x_2^2+x_3^2=(x_1+x_2+x_3)^2-2(x_1x_2+x_2x_3+x_1x_3)=$ $=\sigma_1^2-2\sigma_2$, $s_3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$. Выразим теперь s_k для произвольного k через многочлены s_i, $i<k$. Имеем

$$\sigma_1 s_{k-1}=(x_1+x_2+x_3)\left(x_1^{k-1}+x_2^{k-1}+x_3^{k-1}\right)=s_k+o_3\left(x_1^{k-1}x_2\right).$$

Отсюда

$$s_k=\sigma_1 s_{k-1}-o_3\left(x_1^{k-1}x_2\right).$$

Аналогично,

$$\sigma_2 s_{k-2}=o_3\left(x_1^{k-1}x_2\right)+o_3\left(x_1^{k-2}x_2x_3\right),$$

$$\sigma_3 s_{k-3}=o_3\left(x_1^{k-2}x_2x_3\right).$$

Определяя из двух последних равенств многочлен $o_3\left(x_1^{k-1}x_2\right)$ и подставляя его в предыдущее, будем иметь

$$s_k=\sigma_1 s_{k-1}-\sigma_2 s_{k-2}+\sigma_3 s_{k-3}.$$

В соответствии с предположением индукции степенные суммы s_{k-1}, s_{k-2}, s_{k-3} можно записать в виде многочленов от элементарных симметрических многочленов, следовательно, через них можно выразить и сумму s_k.

2) В § 13 было установлено, что любой орбитальный многочлен вида $o_3\left(x_1^k x_2^l\right)$ выражается через степенные суммы. По только что доказанному, $o_3\left(x_1^k x_2^l\right)$ можно представить в виде многочлена от элементарных симметрических многочленов.

3) Пусть $o_3\left(x_1^k x_2^l x_3^m\right)$ — некоторый орбитальный многочлен, и пусть, например, число m — наименьшее из чисел k, l, m. Тогда имеем

$$o_3\left(x_1^k x_2^l x_3^m\right)=x_1^m x_2^m x_3^m o_3\left(x_1^{k-m}x_2^{l-m}\right)=\sigma_3^m o_3\left(x_1^{k-m}x_2^{l-m}\right),$$

$o_3\left(x_1^{k-m}x_2^{l-m}\right)$ — орбита одночлена с меньшим числом переменных, т. е. этот случай сводится к предыдущим.

Основная теорема о симметрических многочленах для $n=3$ доказана. Для $n=2$ доказательство будет вполне аналогично, но значительно проще. Предлагаем читателю провести его самостоятельно.

◀ Рассмотрим несколько примеров применения основной теоремы о симметрических многочленах.

1. Решить систему

$$x+xy+y=7, \qquad x^2+xy+y^2=13. \tag{1}$$

Выразим симметрические многочлены в левых частях обоих уравнений через $\sigma_1=x+y$ и $\sigma_2=xy$ и введем новые

неизвестные $u=x+y$, $v=xy$. Получим вспомогательную систему

$$u+v=7, \qquad u^2-v=13.$$

Она имеет два решения:

$$u=-5, \ v=12; \qquad u=4, \ v=3.$$

Значит, множество решений исходной системы (1) равно объединению множества решений следующих двух систем:

$$x+y=-5, \ xy=12; \qquad x+y=4, \ xy=3.$$

Множество решений первой из них пусто, а множество решений второй — $\{(1; 3), (3; 1)\}$. Следовательно, множество решений исходной системы (1) есть

$$\varnothing \cup \{(1; 3), (3; 1)\} = \{(1; 3), (3; 1)\}.$$

2. Доказать, что при $a+b+c=0$ справедливо тождество

$$a^3+b^3+c^3=3abc.$$

Выразим симметрический многочлен $a^3+b^3+c^3-3abc$ через элементарные симметрические многочлены $\sigma_1 = a+b+c$, $\sigma_2=ab+ac+bc$, $\sigma_3=abc$. Как было уже установлено при доказательстве теоремы о симметрических многочленах, многочленом от $\sigma_1, \sigma_2, \sigma_3$, который совпадает с суммой $s_3=a^3+b^3+c^3$, является $\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$. Поэтому получим

$$a^3+b^3+c^3-3abc=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3-3\sigma_3=\sigma_1^3-3\sigma_1\sigma_2.$$

Поскольку по условию $\sigma_1=0$, то $a^3+b^3+c^3-3abc$ также равняется 0, откуда и вытекает правильность доказываемого тождества.

3. Составить квадратное уравнение с корнями x_1, x_2, если

$$x_1+x_2=2, \qquad x_1^4+x_2^4=82.$$

Такое уравнение можно составить, использовав теорему Виета. Для этого нужно найти, чему равняется произведение корней. Выражая $x_1^4+x_2^4=s_4$ через элементарные симметрические многочлены, получим $s_4=\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2$. Если в это равенство подставить вместо s_4 и σ_1 их значения, то будем иметь квадратное уравнение для σ_2:

$$2\sigma_2^2-16\sigma_2+66=0.$$

Отсюда $\sigma_2^{(1)}=11$, $\sigma_2^{(2)}=-3$. Следовательно, искомыми уравнениями будут

$$x^2-2x+11=0, \qquad x^2-2x-3=0. \blacktriangleright$$

Наряду с симметрическими многочленами часто приходится иметь дело с четносимметрическими многочленами. *Четносимметрическими* называются многочлены, инвариантные относительно всех четных перестановок. Следовательно, группа инерции четносимметрического многочлена будет содержать знакопеременную группу. Поскольку в симметрической группе S_2 четной будет лишь тождественная перестановка, то каждый многочлен с двумя неизвестными четносимметрический, т. е. в этом случае понятие четносимметричности излишне. Однако уже среди многочленов с тремя неизвестными есть нечетносимметрические, например $x_1+2x_2+3x_3$ (группа инерции этого многочлена единичная).

Понятно, что каждый симметрический многочлен четносимметрический, но не наоборот. Например, знакопеременный многочлен $A(x_1, x_2, \ldots, x_n)$ четносимметрический для любого n, но не симметрический. Четносимметрическим будет, в частности, каждый многочлен, который под действием произвольной транспозиции меняет знак. Многочлены с таким свойством называются *антисимметрическими*. Как было установлено в § 13, многочлен $A(x_1, x_2, \ldots, x_n)$ антисимметрический. Вполне понятно также, что произведение симметрического многочлена на произвольный антисимметрический многочлен снова антисимметрический многочлен. В частности, антисимметрическими будут многочлены вида

$$p(x_1, x_2, \ldots, x_n)\, A(x_1, x_2, \ldots, x_n),$$

где $p(x_1, x_2, \ldots, x_n)$ — любой симметрический многочлен. Можно доказать, что каждый антисимметрический многочлен записывается в виде такого произведения (см. упражнение 7). Ясно, что произведение двух антисимметрических многочленов — многочлен симметрический.

Лемма. *Действуя на произвольный четносимметрический многочлен $f(x_1, x_2, \ldots, x_n)$ нечетными перестановками, будем получать один и тот же многочлен, т. е.*

$$f^{\alpha}(x_1, x_2, \ldots, x_n)=f^{\beta}(x_1, x_2, \ldots, x_n)$$

для любых нечетных перестановок α, β.

Действительно, в этом случае $\alpha \circ \alpha$ и $\beta \circ \alpha$ — четные перестановки и, следовательно,

$$f^{\alpha \circ \alpha} = f^{\beta \circ \alpha}.$$

Действуя на обе части этого равенства перестановкой α^{-1}, получим

$$(f^{\alpha \circ \alpha})^{\alpha^{-1}} = (f^{\beta \circ \alpha})^{\alpha^{-1}}.$$

Поскольку $(f^{\sigma})^{\tau} = f^{\sigma \circ \tau}$ для любых перестановок σ, τ, то

$$f^{(\alpha \circ \alpha) \circ \alpha^{-1}} = f^{(\beta \circ \alpha) \circ \alpha^{-1}}.$$

Используя ассоциативность умножения перестановок, получим

$$f^{\alpha \circ (\alpha \circ \alpha^{-1})} = f^{\beta \circ (\alpha \circ \alpha^{-1})}.$$

В силу определения обратной перестановки имеем $f^{\alpha \circ \varepsilon} = f^{\beta \circ \varepsilon}$, т. е. $f^{\alpha} = f^{\beta}$.

Теорема. *Каждый четносимметрический многочлен может быть представлен, и притом единственным образом, в виде суммы симметрического и антисимметрического многочленов.*

Доказательство. Единственность. Пусть заданный четносимметрический многочлен f представлен в виде

$$f = g + h, \tag{1}$$

где g — некоторый симметрический, h — антисимметрический многочлены. Подействуем на обе части этого равенства какой-нибудь нечетной перестановкой α:

$$f^{\alpha} = g^{\alpha} + h^{\alpha}.$$

Однако, в силу предположений о g и h, $g^{\alpha} = g$, $h^{\alpha} = -h$, т. е.

$$f^{\alpha} = g - h. \tag{2}$$

Складывая и вычитая почленно равенства (1) и (2), получим

$$g = \frac{f + f^{\alpha}}{2}, \qquad h = \frac{f - f^{\alpha}}{2}. \tag{3}$$

Отметим, что в силу ранее доказанной леммы правые части равенств (3) не изменятся, если вместо α взять какую-нибудь другую нечетную перестановку β.

Проведенные рассуждения доказывают, что если разложение (1) возможно, то обязательно для g и h справедливы формулы (3), т. е. g и h, *если существуют, то определены однозначно.*

Существование. Для доказательства существования разложения (1) необходимо проверить, что:

1) $f=\frac{f+f^{\alpha}}{2}+\frac{f-f^{\alpha}}{2}$, где α — некоторая (безразлично какая) нечетная перестановка;

2) $G=\frac{f+f^{\alpha}}{2}$ — симметрический многочлен;

3) $H=\frac{f-f^{\alpha}}{2}$ — антисимметрический многочлен.

Но 1) очевидно, а для доказательства 2) и 3) достаточно заметить следующее. Если β — четная перестановка, то $f^{\beta}=f$, $(f^{\alpha})^{\beta}=f^{\alpha\cdot\beta}=f^{\alpha}$ в силу леммы, так как $\alpha\cdot\beta$ — нечетная перестановка. Поэтому $G^{\beta}=G$, $H^{\beta}=H$. Если же β — нечетная перестановка, то $f^{\beta}=f^{\alpha}$ в силу леммы, а $(f^{\alpha})^{\beta}=f^{\alpha\cdot\beta}=f$, так как $\alpha\cdot\beta$ будет четной перестановкой. Поэтому

$$G^{\beta}=\frac{f^{\alpha}+f}{2}, \qquad H^{\beta}=\frac{f^{\alpha}-f}{2}=-H.$$

Теорема доказана.

В частности, любой многочлен с двумя неизвестными является суммой симметрического и антисимметрического многочленов.

Упражнения

1. Выразить через элементарные симметрические многочлены:

а) $x_1^5+x_2^5$; б) $x_1^4+x_2^4+x_3^4$; в) $o_3(x_1^2x_2)$.

2. Решить системы уравнений:

а) $\sqrt{x}+\sqrt{y}+2=\sqrt{xy}$, $x+y=20$,

б) $x^2+y^2+2x+2y=23$, $x^2+y^2+xy=19$,

в) $x+y=4$, $x^4+y^4=82$.

3. Найти площадь треугольника, зная его периметр, сумму квадратов длин его сторон и сумму кубов длин его сторон.

4. Если некоторый многочлен $f(y_1, y_2)$ обращается в нуль при подстановке x_1+x_2 вместо y_1 и x_1x_2 вместо y_2, то он тождественно равен нулю. Доказать это.

5. *Теорема единственности*: для произвольного симметрического многочлена $f(x_1, x_2)$ существует только один многочлен $g(y_1, y_2)$, такой, что $f(x_1, x_2)=g(\sigma_1, \sigma_2)$. Доказать это утверждение, используя упражнение 4

6. Если $f(x_1, x_2)$ — антисимметрический многочлен, то $f(x_1, x_1)=0$. Доказать это. Сформулировать и доказать аналогичное утверждение для многочленов с тремя переменными.

7. Используя предыдущее упражнение, доказать, что произвольный антисимметрический многочлен $f(x_1, x_2)$ с двумя переменными имеет вид $(x_1-x_2)g(x_1, x_2)$, где $g(x_1, x_2)$ — симметрический многочлен.

8. Функция $f(x_1, x_2, \ldots, x_n)$ от n переменных называется симметрической, если она не изменяет значений при произвольной перестановке аргументов, т. е. для любой перестановки $\sigma \in S_n$ имеем $f(x_{(1)\sigma}, x_{(2)\sigma}, \ldots, x_{(n)\sigma}) = f(x_1, x_2, \ldots, x_n)$. Докажите, что функция

$$f(x_1, x_2, x_3) = \left|\, |x_1 - x_2| + x_1 + x_2 - 2x_3 \right| + |x_1 - x_2| + x_1 + x_2 + 2x_3$$

симметрическая

§ 17. О РЕШЕНИИ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ

1. *Алгебраическим уравнением степени n* называется уравнение вида

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

где старший коэффициент $a_0 \neq 0$.

Простейшие виды алгебраических уравнений — уравнения 1-й и 2-й степени и даже некоторые специальные виды уравнений 3-й степени — математики могли решать еще в древнем Вавилоне примерно 4000 лет тому назад. Правда, в те далекие времена ученые еще не знали современной математической символики и записывали и само уравнение и процесс его решения словами, а не формулами.

2. Произвольное уравнение первой степени

$$ax + b = 0, \quad a \neq 0,$$

всегда имеет, и притом единственное, решение $x = -b/a$.

В школьном курсе алгебры доказывается следующая теорема о решении произвольного квадратного уравнения $ax^2 + bx + c = 0$:

Если число $D = b^2 - 4ac > 0$, то уравнение имеет ровно два корня, которые даются формулой

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}.$$

Если $D = 0$, то корень только один: $x = -\frac{b}{2a}$.

Если же $D < 0$, то корней среди действительных чисел нет.

Математики всегда стараются избежать подобного разделения случаев — их число только увеличилось бы при переходе к уравнениям более высокой степени. Желательна была бы, конечно, формулировка: «Уравнение второй степени имеет два корня». Ее можно достичь, если, с одной стороны, так расширить понятие числа, что было бы возможным извлекать квадратные корни из отрицательных чисел, а с другой — считать некоторые корни «несколько

раз» (ввести понятие кратного корня). И то и другое можно аккуратно сделать.

3. Общее уравнение третьей степени имеет вид

$$Ax^3+Bx^2+Cx+D=0.$$

Разделив обе части этого уравнения на старший коэффициент A — решения от этого, очевидно, не меняются — приходим к уравнению вида

$$x^3+ax^2+bx+c=0.$$

Введением новой неизвестной величины $z=x+\frac{a}{3}$ можно избавиться от слагаемого, содержащего неизвестную во второй степени, т. е. привести уравнение к виду

$$z^3+pz+q=0, \qquad (1)$$

называемому *редуцированным* уравнением третьей степени.

Сведения об истории открытия формулы корней кубического уравнения неполны и противоречивы. По-видимому, первым (около 1515 г.) нашел метод решения кубических уравнений профессор университета в Болонье С. Ферро (1465—1526). Независимо от него (около 1535 г.) этот метод открыл Н. Тарталья (1500—1557). Однако первым опубликовал формулу корней кубического уравнения Дж. Кардано (1501—1576) (его работа вышла в 1545 г.), и поэтому эта формула носит его имя. Отметим, что, возможно, Кардано был знаком с работами Тартальи и Ферро.

В современных обозначениях метод решения уравнения (1) состоит в следующем.

Введем две новые неизвестные u и v; положив $z=u+v$, имеем

$$(u+v)^3+p(u+v)+q=0,$$
$$u^3+v^3+(u+v)(3uv+p)+q=0. \qquad (2)$$

Если неизвестные u, v удовлетворяют системе

$$uv=-\frac{p}{3}, \qquad u^3+v^3=-q, \qquad (3)$$

то они также удовлетворяют уравнению (2). Решить систему (3) очень просто. Возведем первое уравнение в куб и подставим вместо v^3 его выражение из второго уравнения; получим, что $u^3=y$ удовлетворяет квадратному уравнению

$$y^2+qy-\frac{p^3}{27}=0.$$

Следовательно,

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \qquad v^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

и, наконец,

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \quad (4)$$

Это и есть *формула Кардано* для решения редуцированного кубического уравнения (1).

Сразу возникают вопросы:

1) Что делать, если выражение $\frac{q^2}{4} + \frac{p^3}{27} < 0$?

2) Сколько корней имеет кубическое уравнение?

3) Дает ли формула Кардано (4) все решения уравнения (1)?

Вопросы эти взаимосвязаны. Легко, например, убедиться, что уравнение

$$x^3 - 19x + 30 = 0$$

имеет решения —5, 2, 3, а как раз в этом случае

$$\frac{q^2}{4} + \frac{p^2}{27} < 0,$$

так что квадратные корни в формуле Кардано теряют смысл и три указанных корня этой формулой не выражаются.

Все говорит о том, что здесь еще больше, чем в случае квадратных уравнений, нельзя обойтись без введения каких-то «новых чисел», для которых извлечение квадратного корня всегда возможно. Такие числа были постепенно введены на протяжении XVI — XIX вв. Они называются *комплексными числами*. В комплексных числах любое алгебраическое уравнение n-й степени имеет ровно n корней *).

Рассмотрим в качестве примера уравнение

$$x^n - 1 = 0. \quad (5)$$

Оно играет важную роль в теории и понадобится нам в дальнейшем. В поле комплексных чисел это уравнение

*) Прочесть о комплексных числах можно в книгах:

Курош А. Г. Алгебраические уравнения произвольных степеней. — М.: Наука, 1975. — (Популярные лекции по математике).

Курош А. Г. Курс высшей алгебры. — М.: Наука, 1975. (*Примеч. пер.*)

имеет n различных решений, которые называются *корнями n-й степени из единицы*:

$$\rho_0 = 1, \quad \rho_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}, \ \ldots,$$
$$\rho_{n-1} = \cos\frac{2\pi(n-1)}{n} + i\sin\frac{2\pi(n-1)}{n}. \qquad (6)$$

Для записи решений кубического уравнения нужны корни 3-й степени из 1. В соответствии с формулами (6) это будут следующие комплексные числа:

$$\rho_0 = 1, \quad \rho_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$
$$\rho_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Можно показать, что три корня редуцированного кубического уравнения $z^3 + pz + q = 0$ есть

$$z_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$
$$z_2 = \rho\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \rho^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$
$$z_3 = \rho^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \rho\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Здесь буквой ρ обозначен ρ_1 — корень 3-й степени из 1; ρ^2, как нетрудно видеть, равно ρ_2. Это и есть окончательные *формулы Кардано*.

4. В случае уравнений 1-й, 2-й и 3-й степени нам известны формулы, выражающие корни через коэффициенты уравнения при помощи рациональных операций $+$, $-$, $\times$, $:$, операции $\sqrt{\ }$ извлечения квадратного корня (в случае квадратного уравнения), операций $\sqrt{\ }$ и $\sqrt[3]{\ }$ извлечения квадратного и кубического корней (в случае кубического уравнения). Подобные же правила были указаны и для уравнений 4-й степени учеником Дж. Кардано итальянским алгебраистом Л. Феррари (1522—1565). В них также участвуют лишь рациональные операции и операции $\sqrt{\ }$, $\sqrt[3]{\ }$. Все попытки на протяжении почти трех веков (XVI—XVIII) найти подобные правила для уравнений 5-й и более высоких степеней при помощи рациональных операций и операций $\sqrt[m]{\ }$ не увенчались успехом. Постепенно стали подозревать, что, возможно, вообще нельзя выразить корни уравнения n-й степени для $n \geqslant 5$ через

коэффициенты лишь при помощи операций $+$, $-$, $\times$, $:$ и $\sqrt[m]{}$ для произвольных натуральных m, т. е что нельзя свести решение таких уравнений рациональными операциями к последовательному решению уравнений специального вида $y^m = A$. Корни уравнений $y^m = A$, т. е. то, что обычно обозначают через $\sqrt[m]{A}$, принято называть *радикалами*, и поэтому задачу о возможности сведения нахождения корней произвольного уравнения к нахождению уравнений вида $y^m = A$ принято называть *задачей о выражении корней уравнения радикалами*.

Попытки доказать или опровергнуть эту гипотезу особенно участились во второй половине XVIII столетия и привели в начале XIX столетия к доказательству *невозможности решения общего уравнения 5-й и более высоких степеней в радикалах*.

Среди работ XVIII столетия в отмеченном направлении ясностью мысли выделяется мемуар знаменитого французского математика Ж. Л. Лагранжа (1736—1813), озаглавленный «Рассуждения об алгебраическом решении уравнений» (1771—1772). В нем автор подробно и внимательно проанализировал известные методы решения уравнений 2-й, 3-й и 4-й степени в радикалах, чтобы выяснить, как и почему в этих случаях такое решение удается. При этом он отметил следующее обстоятельство: во всех указанных случаях имеются некоторые функции от корней, которые удовлетворяют уравнениям более низкой степени и про которые уже известно, что они решаются в радикалах. Корни исходного уравнения, в свою очередь, могут быть найдены из этих промежуточных функций опять-таки из уравнений, решаемых в радикалах.

Далее, Лагранж исследует вопрос, каким образом находятся подобные функции от корней в известных случаях. Оказалось, что это полиномы $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ от корней $\xi_1, \xi_2, \ldots, \xi_n$, которые при всевозможных перестановках корней — а их число, как известно, равно $n!$ — принимают не $n!$, а меньшее число значений, и даже меньшее, чем n (n — степень исследуемого уравнения). Это произойдет тогда, когда $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ не меняется при *некоторых перестановках* корней.

Вот каким образом перестановки появились в вопросе о решении уравнения в радикалах!

Если функция $\varphi(\xi_1, \ldots, \xi_n)$ от корней принимает только k различных значений $\varphi_1, \ldots, \varphi_k$, то коэффициенты многочлена

$$(y-\varphi_1)\ldots(y-\varphi_k) \equiv y^k + b_1 y^{k-1} + \ldots + b_k$$

по одной известной уже давно теореме — это так называемая *основная теорема о симметрических функциях* — должны рационально выражаться через коэффициенты исследуемого уравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0.$$

◀ Примеры. 1. Пусть $\Delta(\xi_1, \ldots, \xi_n) = \Delta$ — знакопеременная функция

$$\Delta = \prod_{l<m} (\xi_l - \xi_m)$$

от корней уравнения n-й степени. Она принимает при всевозможных перестановках корней лишь два значения Δ и $-\Delta$ в зависимости от того, будет ли перестановка четной или нечетной. Следовательно, дискриминант уравнения $D = \Delta^2$ не меняется при всевозможных перестановках и выражается рационально через коэффициенты исследуемого уравнения. Для квадратного уравнения $ax^2 + bx + c = 0$

$$D = b^2 - 4ac,$$

для редуцированного кубического уравнения $x^3 + px + q = 0$

$$D = -4p^3 - 27q^2.$$

Знакопеременная функция Δ от корней удовлетворяет уравнениям

$$y^2 - (b^2 - 4ac) = 0 \quad \text{и} \quad y^2 + (4p^3 + 27q^2) = 0$$

соответственно. Мы узнаем выражения под квадратным корнем в формуле для решения квадратного уравнения и — с точностью до постоянного множителя — в формуле Кардано.

2. Другой пример появился в упоминавшейся выше работе Лагранжа. Это так называемые *резольвенты Лагранжа*. Мы их рассмотрим, как и сам Лагранж, для случая уравнения 3-й степени. При помощи кубических корней из 1

$$1, \ \rho, \ \rho^2$$

они определяются следующим образом:

$$\begin{aligned} \eta_0 &= \xi_1 + \xi_2 + \xi_3, \\ \eta_1 &= \xi_1 + \rho\xi_2 + \rho^2\xi_3, \\ \eta_2 &= \xi_1 + \rho^2\xi_2 + \rho\xi_3. \end{aligned} \tag{7}$$

Здесь ξ_1, ξ_2, ξ_3 — корни исследуемого кубического уравнения. Обратим внимание на вторую и третью резольвенты. Как нетрудно видеть, при циклической перестановке корней $(\xi_1, \xi_2, \xi_3) \to (\xi_2, \xi_3, \xi_1)$ они лишь умножаются на ρ^2 и ρ соответственно. Следовательно, η_1^3 и η_2^3 выдерживают циклические перестановки и поэтому выражаются рационально через коэффициенты уравнения и через Δ. Соответствующие представления можно подсчитать. Извлечением кубического корня можно получить η_1 и η_2. По теореме Виета $\xi_1 + \xi_2 + \xi_3$ — это коэффициент при z^2 с обратным знаком, т. е. в случае редуцированного кубического уравнения $\eta_0 = 0$. Зная η_0, η_1, η_2, из системы линейных уравнений (7), можно получить ξ_1, ξ_2, ξ_3. Если осуществить указанные вычисления, то можно убедиться, что ξ_1, ξ_2, ξ_3 вычисляются по формулам Кардано. ▶

Аналогично, только технически более сложно, можно получить решение в радикалах уравнения 4-й степени. Что же касается уравнения 5-й степени, то аналогичное сведение к уравнениям низших степеней получить не удалось. Однако Лагранж не исключал его возможности.

Что такое понижение принципиально неосуществимо, показал в 1799 г. в работе «Общая теория уравнений, в которой доказывается невозможность алгебраического решения общих уравнений выше четвертой степени» итальянский математик П. Руффини (1765—1822). Однако в его доказательстве содержались пробелы, которые ему не удалось устранить. Аккуратное доказательство было дано лишь в 1826 г. в работе норвежского математика Н. Г. Абеля (1802—1829) «Доказательство невозможности алгебраической разрешимости уравнений, степень которых превышает четвертую».

Глубокую причину несуществования функций от корней, удовлетворяющих уравнениям более низкой степени, чем рассматриваемое (исключение составляет всегда знакопеременная функция, удовлетворяющая квадратному уравнению) вскрыл гениальный французский математик Эварист Галуа (1811—1832). Галуа сопоставил каждому уравнению группу тех перестановок его корней, которые не меняют значения всех полиномов от корней с коэффициентами, зависящими рационально от коэффициентов заданного уравнения. Эту группу называют теперь *группой Галуа* рассматриваемого уравнения.

Понятие группы Галуа уравнения можно ввести следующим образом. Пусть $f(x) = 0$ — алгебраическое уравнение некоторой степени n, $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$,

$a_0 \neq 0$ (левая часть этого уравнения) — полином степени n. Коэффициенты полинома — числа $a_0, a_1, \ldots, a_n$ должны принадлежать одновременно какому-либо *числовому полю* — непустому множеству чисел, замкнутому относительно операций сложения, умножения, вычитания и деления на число, отличное от 0. Числовым полем является, например, множество $\mathbf{Q}$ всех рациональных чисел. Поскольку необходимые понятия вводятся для всех числовых полей единообразно, достаточно рассмотреть лишь одно из них. Поэтому мы будем считать, что коэффициенты многочлена $f(x)$ — рациональные числа. Кроме того, можно предполагать (это доказывается в курсах алгебры), что все корни многочлена $f(x)$ — различны, т. е. уравнение $f(x)=0$ имеет n различных, вообще говоря, комплексных корней $\xi_1, \xi_2, \ldots, \xi_n$. *Рациональным отношением* между корнями $\xi_1, \xi_2, \ldots, \xi_n$ называется всякое равенство вида

$$\sum_{(i_1, i_2, \ldots, i_n)} a_{i_1 i_2 \ldots i_n} \xi_1^{i_1} \xi_2^{i_2} \ldots \xi_n^{i_n} = 0, \qquad (8)$$

где $\sum$ — знак суммирования, сумма, стоящая в левой части этого равенства, берется по каким-то наборам показателей $i_1, i_2, \ldots, i_n$, а все коэффициенты $a_{i_1 i_2 \ldots i_n}$ — рациональные числа. Иными словами, в левой части рационального отношения (8) стоит некоторый многочлен от $\xi_1, \xi_2, \ldots, \xi_n$ с рациональными коэффициентами. Множество всех рациональных отношений между корнями уравнения $f(x)=0$ зависит только от многочлена $f(x)$. Понятно, что почленная сумма и почленное произведение рациональных отношений между корнями некоторого многочлена тоже будут рациональными отношениями между его корнями. Поскольку пример ненулевого рационального отношения легко указать для любого уравнения $f(x)=0$, отсюда получаем, что произвольному уравнению $f(x)=0$ соответствует бесконечное множество рациональных отношений между его корнями.

Пусть теперь

$$\alpha = \begin{pmatrix} \xi_1 & \xi_2 & \ldots & \xi_n \\ \xi_{k_1} & \xi_{k_2} & \ldots & \xi_{k_n} \end{pmatrix}$$

— некоторая перестановка на множестве корней уравнения $f(x)=0$. Подействуем этой перестановкой на левую часть выражения (8). Каждый одночлен $a_{i_1 i_2 \ldots i_n} \xi_1^{i_1} \xi_2^{i_2} \ldots \xi_n^{i_n}$ под действием перестановки преобразуется в одночлен $a_{i_1 i_2 \ldots i_n} \xi_{k_1}^{i_1} \xi_{k_2}^{i_2} \ldots \xi_{k_n}^{i_n}$ (коэффициенты при всех одночленах

остаются неизменными). Левая часть соотношения (8) преобразуется в следующее выражение:

$$\sum_{(i_1, i_2, \ldots, i_n)} a_{i_1 i_2 \ldots i_n} \xi_{k_1}^{i_1} \xi_{k_2}^{i_2} \ldots \xi_{k_n}^{i_n}.$$

Это число может оказаться отличным от нуля. Все перестановки из симметрической группы на множестве корней $\xi_1, \xi_2, \ldots, \xi_n$ уравнения $f(x)=0$ можно разделить на две части — те, что сохраняют рациональное отношение (8), и те, что нарушают его. Если перестановки α и β сохраняют рациональное отношение (8), то очевидно, что их произведение $\alpha \circ \beta$ и обратная перестановка к каждой из них также будут преобразовывать это равенство в верхнее соотношение такого же вида. Иными словами, множество всевозможных перестановок, сохраняющих соотношение (8) (поскольку оно не пустое!), образует группу. Эта группа и называется *группой Галуа* уравнения $f(x)=0$.

По свойствам этой группы Галуа можно определить, будет ли данное уравнение разрешимо в радикалах или нет. Полученный признак содержит в виде частных случаев все ранее известные сведения о разрешимости или неразрешимости в радикалах алгебраических уравнений.

Но не исключается, что некоторые уравнения с числовыми коэффициентами разрешимы в радикалах. Возможно это или нет, устанавливается опять-таки на основании признака, найденного Галуа.

Исследование свойств групп Галуа выходит за рамки нашего изложения. Отметим только, что если группа Галуа данного уравнения является абелевой, то уравнение разрешимо в радикалах. Разрешимыми в радикалах будут уравнения, группа Галуа которых является одной из групп диэдра, группой симметрий тетраэдра и куба. Это примеры так называемых *разрешимых групп*, т. е. групп Галуа уравнений, разрешимых в радикалах. Наиболее «маленьким» примером *неразрешимой группы* является знакопеременная группа A_5, состоящая из 60 перестановок; неразрешимой является также и содержащая ее группа S_5. Можно сказать, что в неразрешимости общего уравнения 5-й степени в радикалах «виновны» именно эти группы: среди уравнений 5-й степени имеются такие, группа Галуа которых совпадает с A_5 или S_5. Примером такого уравнения является

$$x^5 - 10x - 2 = 0.$$

Поскольку группа Галуа уравнения является столь важной его характеристикой, возникает вопрос, как же строить эту группу по уравнению? Оказывается, что нет необходимости проверять, выдерживают ли все рациональные отношения от корней уравнения $f(x)=0$ данную перестановку его корней. Достаточно ограничиться такой проверкой для конечной и вполне обозримой части этих отношений. С доказательством последнего и других упомянутых здесь утверждений можно познакомиться по одной из книг, посвященных изложению теории Галуа и указанных в списке литературы.

Упражнения

1. Используя дискриминант D кубического уравнения, невозможно установить, все корни этого уравнения совпадают, или же совпадают лишь два из них. Приведите пример выражения, составленного из корней данного уравнения, которое позволяло бы это делать.

2. Доказать, что если α — корень многочлена $f(x)$, т. е. $f(\alpha)=0$, то $f(x)$ делится на $x-\alpha$ без остатка, т. е. найдется такой многочлен $g(x)$, что $f(x)=(x-\alpha)g(x)$.

3. Пусть $\xi_1, \xi_2, \ldots, \xi_n$ — корни уравнения $f(x)=0$, где $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$. Доказать, что имеют место равенства

$$\sigma_1(\xi_1, \xi_2, \ldots, \xi_n)=-a_1,$$
$$\sigma_2(\xi_1, \xi_2, \ldots, \xi_n)=a_2,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_n(\xi_1, \xi_2, \ldots, \xi_n)=(-1)^n a_n.$$

Это утверждение при $n=2$ читателям хорошо известно как *теорема Виета*. В общем случае оно тоже так называется.

4. Пусть $g(\xi_1, \xi_2, \ldots, \xi_n)$ — некоторый симметрический многочлен с рациональными коэффициентами от корней $\xi_1, \xi_2, \ldots, \xi_n$ уравнения $f(x)=0$. Доказать, что существует такое рациональное число c, для которого выражение

$$g(\xi_1, \xi_2, \ldots, \xi_n)+c=0$$

будет рациональным соотношением между корнями уравнения $f(x)=0$.

5. Привести примеры числовых полей, отличных от поля рациональных чисел Q. Проверить, что всевозможные числа вида

$$a+b\sqrt{3}, \qquad a, b\in \mathbf{Q},$$

образуют числовое поле.

6. Доказать, что если квадратный корень из дискриминанта многочлена $f(x)$ является рациональным числом, то группа Галуа этого многочлена целиком состоит из четных перестановок.

§ 18. ИГРА «В ПЯТНАДЦАТЬ»

Теория перестановок нашла применение и при математическом анализе многих популярных игр. Например, одно время очень популярной была почти забытая теперь

игра «в пятнадцать». И «виноваты» в том, что она забыта, математики, потому что они строго доказали, что определенные позиции этой игры являются выигрышными, а остальные — нет. Здесь мы приведем доказательство этого факта, использовав теорию перестановок.

Сначала коротко опишем смысл игры.

В плоской квадратной коробке размещены 15 одинаковых фишек квадратной формы, одно место остается свободным. Фишки занумерованы числами от 1 до 15 и размещены в определенном порядке (например, так, как на рис. 34 *а*).

Не вынимая фишек из коробки, а лишь передвигая друг за другом на свободное место, нужно разместить их в порядке возрастания номеров так, как на рис. 34 *б*.

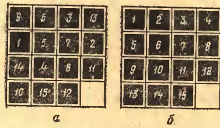


Рис. 34

Оказывается, что прийти к такому размещению фишек — будем называть его *стандартным* — можно не всегда. Существуют позиции, от которых этот переход осуществить нельзя.

Договоримся называть *начальными* те размещения фишек в коробке, в которых свободное место остается в правом нижнем углу. В другом случае будем говорить просто про *позицию* игры.

С каждым размещением фишек в коробке можно связать определенную перестановку на множестве $M = \{1, 2, 3, \ldots, 15, 16\}$, считая, что свободное место — это фиктивная фишка с номером 16. Для этого занумеруем места, которые могут занимать фишки, числами от 1 до 16 так, чтобы порядок нумерации совпадал с порядком стандартного размещения фишек. Следовательно, *каждое размещение фишек однозначно характеризуется перестановкой на множестве M, первый ряд которой составляют номера мест, а второй — номера фишек, которые на этих местах стоят.* Например, размещение фишек на рис. 34 *а*

описывается перестановкой

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 9 & 6 & 3 & 13 & 1 & 5 & 7 & 2 & 14 & 4 & 8 & 11 & 10 & 15 & 12 & 16 \end{pmatrix},$$

а размещение фишек на рис. 34 *б* — единичной перестановкой.

Начальные размещения можно однозначно описывать перестановками на множестве $M_1 = \{1, 2, \ldots, 15\}$, так как для них фиктивная фишка «стоит» на месте с номером 16. Переход от позиции, которая характеризуется перестановкой φ, к позиции, которая характеризуется перестановкой ψ, если он возможен, осуществляется за несколько «ходов», причем каждый ход — это передвигание на свободное место какой-нибудь соседней фишки. Если свободным является i-е место, а фишка, которая будет передвигаться, имеет номер a_j и стоит на j-м месте, то после перемещения эта фишка будет стоять на i-м месте, а j-е место освободится. Значит, за один ход от размещения

$$\varphi = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & 16 \\ a_1 & a_2 & \ldots & 16 & \ldots & a_j & \ldots & a_{16} \end{pmatrix}$$

мы переходим к размещению

$$\varphi_1 = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & 16 \\ a_1 & a_2 & \ldots & a_j & \ldots & 16 & \ldots & a_{16} \end{pmatrix}.$$

Следовательно, перестановку φ мы умножаем на транспозицию

$$\delta_1 = (a_j,\ 16) = \begin{pmatrix} 1 & 2 & \ldots & a_j & \ldots & 15 & 16 \\ 1 & 2 & \ldots & 16 & \ldots & 15 & a_j \end{pmatrix}$$

и имеем равенство $\varphi_1 = \varphi \cdot \delta_1$.

Если от позиции, которая описывается перестановкой φ_1, можно перейти к новой за один ход, то найдется такая транспозиция δ_2, что перестановка φ_2, которая отвечает новой позиции, будет связана с φ_1 равенством

$$\varphi_2 = \varphi_1 \cdot \delta_2.$$

Допустим теперь, что для перехода от позиции φ к позиции ψ нужно сделать k ходов. Это означает, что существуют такие транспозиции $\delta_1, \delta_2, \ldots, \delta_k$ вида $(i, 16)$, для которых справедливо равенство

$$\psi = \varphi \cdot \delta_1 \cdot \delta_2 \cdot \ldots \cdot \delta_k.$$

На свободное место каждый раз передвигается соседняя фишка, а это накладывает определенные ограничения на произведение $\delta_1 \circ \delta_2 \circ \ldots \circ \delta_k$. *Если от начального размещения* φ *удается перейти к стандартному, то можно подобрать такие транспозиции* $\delta_1, \delta_2, \ldots, \delta_s$ *отмеченного вида, чтобы выполнялось равенство*

$$\varphi \circ \delta_s \circ \delta_{s-1} \circ \ldots \circ \delta_1 = \varepsilon,$$

откуда $\varphi = \delta_1^{-1} \circ \delta_2^{-1} \circ \ldots \circ \delta_s^{-1} = \delta_1 \circ \delta_2 \circ \ldots \circ \delta_s$. Но такое произведение не может быть произвольным, так как последовательности транспозиций $\delta_1, \delta_2, \ldots, \delta_s$ отвечает последовательность ходов, причем на свободное место каждый раз передвигается соседняя фишка.

Покажем сначала, что *когда от начального положения* φ *можно перейти к стандартному, то перестановка* φ *— четная.*

Занумеруем ряды и столбцы, составленные из фишек так, как на рис. 35. При каждом перемещении фишки на свободное место (переставлении ее с фиктивной) сумма номеров ряда и столбца, в которых стоит фиктивная фишка, увеличивается или уменьшается на единицу. Действительно, место каждой фишки однозначно характеризуется парой чисел (i, j) $(i, j = 1, 2, 3, 4)$. Если фиктивная фишка «стоит» на месте (i, j), то очередной ход можно сделать четырьмя способами:

	1	2	3	4
1				
2			(2,3)	
3				
4		(4,2)		

Рис. 35

$$(i, j) \to (i-1, j) \quad (i \neq 1),$$
$$(i, j) \to (i+1, j) \quad (i \neq 4),$$
$$(i, j) \to (i, j-1) \quad (j \neq 1),$$
$$(i, j) \to (i, j+1) \quad (j \neq 4),$$

или лишь двумя или тремя из них, если фиктивная фишка «стоит» возле стенки коробки. В каждом из этих случаев сумма $i + j$ заменяется на $i + j + 1$ или на $i + j - 1$, т. е. увеличивается или уменьшается на единицу.

Пусть теперь задана некоторая начальная позиция φ. Пустое место в этой позиции по нашей нумерации имеет «номер» (4, 4). Если после некоторого количества передвижений фишек на свободное место перейдем к стандартной позиции, то фиктивная фишка вновь будет иметь такой номер. Поскольку на каждом шаге (при каждой транспозиции) четность суммы номеров ряда и столбца,

в которых «стоит» фиктивная фишка, изменяется, она может вернуться на место (4, 4) лишь через четное число ходов. Следовательно, перестановка φ раскладывается в произведение четного числа транспозиций, т. е. она четна.

Оказывается, что условие четности перестановки, которая характеризует начальное расположение фишек, является и **достаточным** для того, чтобы от этой позиции можно было перейти к стандартной. Доказывать это утверждение для всех четных перестановок не нужно, потому что, как легко понять, когда от каждой из позиций, которые описываются перестановками φ и ψ, можно перейти к стандартной, то это удается осуществить и от позиции $\varphi \circ \psi$. Поэтому достаточно убедиться в этом лишь для таких перестановок, в произведения которых раскладывается каждая четная перестановка. Возьмем, например, перестановки

$$(1,\ 2,\ 3),\quad (1,\ 2,\ 4),\quad (1,\ 2,\ 5),\quad \ldots,\quad (1,\ 2,\ 15). \qquad (1)$$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Рис. 36

Все фишки в коробке, кроме тех, которые стоят на первом и втором местах, можно «связать» в одну цепь, которая может двигаться так, чтобы взаимное размещение звеньев цепи не изменялось (если не учитывать свободного места, которое может двигаться вдоль цепи). Для этого достаточно представить себе, что в коробке поставлены внутренние стенки, например, так, как это сделано на рис. 36. Фишки могут двигаться вдоль «стенок» по часовой стрелке или против нее. Каждая фишка, которая входит в цепь, после определенного числа шагов может стать на место с номером 3.

Пусть размещение характеризуется циклом $(1, 2, k)$, т. е. в коробке фишка с номером 2 стоит на первом месте, фишка с номером k — на втором месте, фишка с номером 1 — на k-м месте $(3 \leqslant k \leqslant 15)$, а все остальные — на своих местах. Делая определенное число перемещений звеньев цепи, мы можем фишку с номером 1 поставить на 3-е место. После этого, перемещая фиктивную фишку вдоль цепи в противоположном направлении, освободим место с номером 7. Теперь можно, переставляя лишь фишки, что стоят на местах с номерами 1, 2, 3, 5, 6, 7, достичь того, чтобы фишки с номером 1 и 2 стали на свои места, с номером k — на третье место, а остальные не изменили позиций. Это видно из схемы последовательного

перемещения фишек, приведенной на рис. 37. На этой схеме $\circ$ и $\times$ обозначают фишки, номера которых для нас несущественны.

В результате таких перемещений изменился порядок размещения лишь трех фишек. Фишку с номером k можно теперь включить в цепь. Перемещая по цепи, поставим ее на место с номером k. При этом все остальные фишки из цепи займут начальное положение. Осталось лишь поставить фиктивную фишку на последнее место, и мы получим стандартное размещение.

2	k	1
×	o	

→

2		k
×	o	1

→

×	2	k
o	1	

→

×	1	2
o		k

→

1	2	k
×	o	

Рис. 37

Докажем теперь, что *каждая четная перестановка раскладывается в произведение циклов из ряда* (1). Действительно, каждая четная перестановка α раскладывается в произведение четного числа транспозиций:

$$\alpha = \delta_1 \circ \delta_2 \circ \ldots \circ \delta_{2k-1} \circ \delta_{2k}. \qquad (2)$$

Если $\sigma = (1, 2)$, то в силу равенства $\sigma^2 = \varepsilon$ можно написать

$$\alpha = \delta_1 \circ \sigma \circ \sigma \circ \delta_2 \circ \delta_3 \circ \sigma \circ \sigma \circ \delta_4 \circ \ldots \circ \delta_{2k-1} \circ \sigma \circ \sigma \circ \delta_{2k} =$$
$$= (\delta_1 \circ \sigma) \circ (\sigma \circ \delta_2) \circ (\delta_3 \circ \sigma) \circ (\sigma \circ \delta_4) \circ \ldots \circ (\delta_{2k-1} \circ \sigma) \circ (\sigma \circ \delta_{2k}).$$

Для завершения доказательства достаточно показать, что для любой транспозиции (i, j) оба произведения $(i, j) \circ (1, 2)$ и $(1, 2) \circ (i, j)$ можно разложить в произведение циклов из ряда (1). А этот факт действительно имеет место, как показывают следующие легко проверяемые равенства:

$$(1, 2) \circ (i, j) = (i, j) \circ (1, 2) =$$
$$= (1, 2, j) \circ (1, 2, i) \circ (1, 2, i) \circ (1, 2, j), \quad \text{если} \quad i, j > 2,$$
$$(1, 2) \circ (1, j) = (2, j) \circ (1, 2) = (1, 2, j), \qquad \text{если } j > 2,$$
$$(1, 2) \circ (2, j) = (1, j) \circ (1, 2) = (1, 2, j) \circ (1, 2, j), \quad \text{если } j > 2.$$

Если одно из δ_k в разложении (2) равно $(1, 2)$, то соответствующее произведение на σ будет тождественной перестановкой и его можно не учитывать.

Упражнения

1. Как практически осуществлять переход к стандартной позиции от размещений, которые характеризуются четной перестановкой?

2. Доказать, что каждая четная перестановка на множестве $M=\{1, 2, \dots, n\}$ раскладывается в произведение таких циклов длины 3: $(1, 2, 3)$, $(2, 3, 4)$, ..., $(n-2, n-1, n)$.

3. Разложить в произведение циклов вида $(1, 2, k)$ перестановки

$$\varphi=(1, 2, 3)\circ(7, 5)\circ(4, 6, 9, 8),$$
$$\psi=(1, 2, 3, 4)\circ(8, 7, 5, 6).$$

4. Можно ли перейти к стандартному размещению от начальных позиций, заданных перестановками

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\\ 8 & 7 & 6 & 5 & 1 & 2 & 4 & 3 & 13 & 15 & 11 & 10 & 14 & 12 & 9\end{pmatrix},$$
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\\ 6 & 3 & 4 & 5 & 2 & 1 & 15 & 10 & 13 & 12 & 11 & 14 & 9 & 8 & 7\end{pmatrix}?$$

5. Если позиция характеризуется нечетной перестановкой, то от нее можно перейти к размещению, которое отличается от стандартного порядком двух последних фишек. Доказать это.

6. На фишках для игры «в пятнадцать» вместо чисел написаны буквы и, г, р, а, в, п, я, т, н, а, д, ц, а, т, ь. Перемещая фишки, как в игре в «пятнадцать», от каждого размещения можно перейти к такому, когда буквы на фишках образуют фразу «игра в пятнадцать». Доказать это.

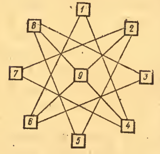


Рис. 38

7. Игра «хамелеон» проводится на «доске» с девятью клетками, которые соединены прямолинейными отрезками (рис. 38). На восьми фишках выписаны буквы х, а, м, е, л, е, о, н. Фишки в случайном порядке расставлены на клетках, расположенных в вершинах многоугольника. Цель игры состоит в том, чтобы, передвигая фишки по соединительным отрезкам, разместить их в правильном порядке, т. е. так, чтобы при чтении по часовой стрелке, начиная с клетки 1, получилось слово «хамелеон». Докажите, что прийти к правильному размещению фишек можно при любом их начальном расположении.

8. Доказать, что теория игры «в пятнадцать» остается в силе и для игры «в восемь», правила которой такие же, как и при игре «в пятнадцать», но здесь 8 фишек с номерами 1, 2, 3, 4, 5, 6, 7, 8 перемещаются в квадрате с 9 клетками.

9. Пусть на фишках для игры «хамелеон» вместо букв выписаны числа 1, 2, 3, 4, 5, 6, 7, 8. Правила игры остаются прежними. Доказать, что полученная таким образом игра в точности совпадает с игрой «в восемь».

10. По аналогии с игрой «в 15» проведите исследование игры «в двадцать четыре».

§ 19. ПЕРЕСТАНОВОЧНЫЕ КОНСТРУКЦИИ

Нам понадобится в этом параграфе операция прямого произведения множеств. *Прямым произведением множеств* M_1, M_2 называется множество всевозможных упорядоченных пар вида (m_1, m_2), первая компонента которых является элементом множества M_1, а вторая — элементом множества M_2. Прямое произведение множеств M_1 и M_2 обозначается символом $M_1 \times M_2$. Например, имеем

$$\{1, 2, 3\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\},$$
$$\{1, 2\} \times \{2, 3, 4\} = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}.$$

Понятно, что для конечных множеств M_1 и M_2 имеет место равенство

$$|M_1 \times M_2| = |M_1| \times |M_2|.$$

Наглядно прямое произведение множеств удобно изображать в виде прямоугольной решетки: элементам множеств M_1 и M_2 ставятся в соответствие точки на «координатных осях» M_1, M_2 (рис. 39), через эти точки проводят соответственно горизонтальные и вертикальные прямые, образующие прямоугольную решетку, и узлам этой решетки соответствуют элементы прямого произведения. Мы уже использовали такой способ изображения, например, в § 12 (рис. 32). Будем рассматривать только прямые произведения множеств натуральных чисел. Условимся располагать элементы прямого произведения $\{1, 2, \ldots, k\} \times \{1, 2, \ldots, l\}$ в следующем порядке:



Рис. 39

$$(1, 1), (1, 2), \ldots, (1, l), (2, 1), (2, 2), \ldots$$
$$\ldots, (2, l), \ldots, (k, 1), (k, 2), \ldots, (k, l), \qquad (1)$$

т. е. упорядочим по возрастанию вначале первые компоненты, а при равных первых компонентах — вторые, и тоже по возрастанию. (Такой порядок называется лексикографическим.)

Рассмотрим теперь конструкции, которые позволяют по перестановкам на множествах M_1 и M_2 строить перестановки на множествах $M_1 \cup M_2$ и $M_1 \times M_2$. Самая простая среди них — это так называемая *сумма перестановок*.

Пусть множества M_1 и M_2 не имеют общих элементов, т. е. $M_1 \cap M_2 = \varnothing$, и α — некоторая перестановка на множестве M_1, а β — перестановка на множестве M_2. *Суммой* (*прямой*) *перестановок* α и β называется перестановка на множестве $M_1 \cup M_2$, которая на элементы M_1 действует так, как α, а на элементы M_2 — так, как β. Мы будем обозначать эту перестановку символом $\alpha \oplus \beta$. Согласно определению имеем, что $\alpha \oplus \beta$ действует на произвольный элемент $m \in M_1 \cup M_2$ так:

$$(m)(\alpha \oplus \beta) = \begin{cases} (m)\alpha, & \text{если} \quad m \in M_1, \\ (m)\beta, & \text{если} \quad m \in M_2 \end{cases}$$

◀ Примеры. 1. Пусть $M_1 = \{1, 2, 3, 4\}$, $M_2 = \{5, 6, 7, 8\}$ и на множествах M_1, M_2 заданы соответственно перестановки

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 \end{pmatrix}.$$

Тогда

$$\alpha \oplus \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 3 & 8 & 7 & 6 & 5 \end{pmatrix}.$$

2. Согласно доказанной в § 5 теореме, любую перестановку можно разложить в произведение взаимно простых циклов. Понятие циклической перестановки мы рассматривали в двух различных смыслах — это собственно циклические перестановки и их расширения на бо́льшие множества. В формулировке теоремы понятие цикла употребляется во втором смысле, т. е. все циклические перестановки в разложении

$$\varphi = \bar{\varphi}_1 \circ \bar{\varphi}_2 \circ \ldots \circ \bar{\varphi}_s$$

перестановки φ в произведение взаимно простых циклов — это перестановки на множестве M, являющиеся расширениями циклов $\varphi_1, \varphi_2, \ldots, \varphi_s$, которые действуют на непересекающихся подмножествах $M_1, M_2, \ldots, M_s$ множества M. Применяя $s-1$ раз конструкцию прямой суммы к циклам $\varphi_1, \varphi_2, \ldots, \varphi_s$, получим равенство

$$\varphi = \varphi_1 \oplus \varphi_2 \oplus \ldots \oplus \varphi_s.$$

Из этого примера понятно, что сумму перестановок α, β можно получить также следующим образом: рассмотреть расширения $\bar{\alpha}$ и $\bar{\beta}$ этих перестановок на множество $M_1 \cup M_2$ и перемножить их. Итак, $\alpha \oplus \beta = \bar{\alpha} \cdot \bar{\beta}$. ▶

Рассмотрим теперь несколько более сложную конструкцию, которая называется *прямым произведением пере-*

становок. С помощью этой конструкции по перестановкам α и β на множествах M_1 и M_2 соответственно строится перестановка на прямом произведении $M_1 \times M_2$. Эта перестановка действует на произвольный элемент (m_1, m_2) из прямого произведения $M_1 \times M_2$ так, что перестановка α изменяет первую компоненту пары, а перестановка β — ее вторую компоненту. Мы будем обозначать так построенную перестановку символом $\alpha \times \beta$. Таким образом, для произвольной пары $(m_1, m_2) \in M_1 \times M_2$

$$(m_1, m_2)(\alpha \times \beta) = ((m_1)\alpha, (m_2)\beta).$$

◀ Примеры. 3. Пусть

$$\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Тогда $\alpha \times \beta$ — перестановка на множестве $\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$. Согласно определению, имеем

$$(1, 1)(\alpha \times \beta) = ((1)\alpha, (1)\beta) = (2, 2),$$
$$(1, 2)(\alpha \times \beta) = ((1)\alpha, (2)\beta) = (2, 3),$$
$$(1, 3)(\alpha \times \beta) = ((1)\alpha, (3)\beta) = (2, 1),$$
$$(2, 1)(\alpha \times \beta) = ((2)\alpha, (1)\beta) = (1, 2),$$
$$(2, 2)(\alpha \times \beta) = ((2)\alpha, (2)\beta) = (1, 3),$$
$$(2, 3)(\alpha \times \beta) = ((2)\alpha, (3)\beta) = (1, 1).$$

Таким образом, перестановка $\alpha \times \beta$ имеет следующую таблицу значений:

$$\begin{pmatrix} (1, 1) & (1, 2), & (1, 3) & (2, 1) & (2, 2) & (2, 3) \\ (2, 2) & (2, 3), & (2, 1) & (1, 2) & (1, 3) & (1, 1) \end{pmatrix}. \qquad (2)$$

Легко понять, как построить эту таблицу непосредственно по таблицам перестановок α и β. Ранее мы оговорили, что все перестановки будут рассматриваться над начальными отрезками натуральных чисел. Перестановке $\alpha \times \beta$ можно поставить в соответствие перестановку на множестве $\{1, 2, 3, 4, 5, 6\}$, занумеровав элементы прямого произведения следующим образом:

1	2	3	4	5	6
(1, 1)	(1, 2)	(1, 3)	(2, 1)	(2, 2)	(2, 3)

Получим следующую перестановку:]

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

Эту перестановку можно сконструировать в два этапа. А именно: разбиваем множество $\{1, 2, 3, 4, 5, 6\}$ на две

одинаковые части $\{1, 2, 3\}\{4, 5, 6\}$ и на каждой из этих частей производим такую же перестановку, как и β. Получим перестановку

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}.$$

Затем переставляем эти части во второй строке таблицы, не измеияя порядок элемеитов в них.

Конечно, переход от записи $\alpha\times\beta$ в виде (2) к записи (3) зависит от выбора иумерации. Но если иумерацию считать фиксироваииой, то любая из этих таблиц однозиачио восстанавливается по другой. Поскольку приходится использовать как одиу из них, так и другую, условимся элементы множества $M_1\times M_2$ иумеровать согласио порядку (1).

4. Перестановку

$$\gamma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 7 & 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix},$$

естествеиио сопоставлять произведеиию перестаиовок

$$\alpha=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ и } \beta=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

В самом деле, перестановка $\alpha\times\beta$ задается таблицей

$$\begin{pmatrix} (1,1) & (1,2) & (1,3) & (2,1) & (2,2) & (2,3) & (3,1) & (3,2) & (3,3) \\ (3,2) & (3,3) & (3,1) & (2,2) & (2,3) & (2,1) & (1,2) & (1,3) & (1,1) \end{pmatrix},$$

которой при задании нумерации элемеитов прямого произведеиия $\{1, 2, 3\}\times\{1, 2, 3\}$ соответственно упорядочеиию (1) отвечает как раз таблица γ. ▶

С помощью второй конструкции можио строить перестаиовки на прямом произведеиии $M_1\times M_2$ миожеств M_1, M_2, примеияя ее ие к двум перестаиовкам, а к $(k+1)$, где $k=|M_1|$. Пусть α — некоторая перестановка иа миожестве M_1, а $\beta_1, \beta_2, \ldots, \beta_k$ — перестаиовки иа миожестве M_2. Миожество $M_1\times M_2$ разбивается иа k иепересекающихся частей следующим образом:

$$M_1\times M_2=\{(1, 1), (1, 2), \ldots, (1, l)\}\cup\{(2, 1), (2, 2), \ldots \\ \ldots, (2, l)\}\cup\ldots\cup\{(k, 1), (k, 2), \ldots, (k, l)\}$$

$(l=|M_2|)$. Преобразование, определяемое элемеитами α, β_1, $\beta_2, \ldots, \beta_k$, действует на произвольную пару (i, j) иа $M_1\times M_2$ так, что иа первую компонеиту пары действует перестаиовка α, а иа вторую — перестановка β_i $(1\leqslant i\leqslant k)$. Иными словами, иа первые коордииаты всех пар из $M_1\times M_2$ действует перестановка α, на вторые координаты пар из

множества $\{(1, 1), (1, 2), \ldots, (1, l)\}$ — перестановка β_1, на вторые координаты пар из множества $\{(2, 1), (2, 2), \ldots \ldots, (2, l)\}$ — перестановка β_2 и т. д.

Будем называть так построенную перестановку *сплетением перестановок* $\beta_1, \beta_2, \ldots, \beta_k$ с помощью перестановки α и обозначать символом

$$[\alpha; \beta_1, \beta_2, \ldots, \beta_k].$$

Итак, согласно определению, действие сплетения перестановок $\beta_1, \beta_2, \ldots, \beta_k$ с помощью перестановки α на произвольный элемент $(i, j) \in M_1 \times M_2$ определяется равенством

$$(i, j)[\alpha; \beta_1, \beta_2, \ldots, \beta_k] = ((i)\alpha, (j)\beta_i).$$

То, что прямая сумма и прямое произведение перестановок — снова перестановка, вполне понятно и не требует дополнительных проверок. Для сплетения это совсем не очевидно. Поэтому покажем, что для произвольных перестановок $\alpha; \beta_1, \beta_2, \ldots, \beta_k$ сплетение $[\alpha; \beta_1, \beta_2, \ldots, \beta_k]$ является перестановкой на множестве $M_1 \times M_2$.

Поскольку M_1 и M_2 — конечные множества, то достаточно проверить, что преобразование $[\alpha; \beta_1, \beta_2, \ldots, \beta_k]$ инъективно. Пусть (i, j), (i', j') — различные пары из прямого произведения $M_1 \times M_2$. Это означает, что выполнено по крайней мере одно из неравенств $i \neq i'$ или $j \neq j'$. Если $i \neq i'$, то $(i)\alpha \neq (i')\alpha$ и, независимо от того равны между собой числа j, j' или нет, пары $((i)\alpha, (j)\beta_i)$ и $((i')\alpha, (j')\beta_i)$ между собой различны. Пусть теперь $i = i'$. Тогда $j \neq j'$ и пары $((i)\alpha, (j)\beta_i)$, $((i)\alpha, (j')\beta_i)$ между собой различны, поскольку $(j)\beta_i \neq (j')\beta_i$. Итак, для произвольных различных пар $(i, j), (i', j')$ из $M_1 \times M_2$ имеем

$$(i, j)[\alpha; \beta_1, \beta_2, \ldots, \beta_k] \neq (i', j')[\alpha; \beta_1, \beta_2, \ldots, \beta_k],$$

т. е. сплетение перестановок $[\alpha; \beta_1, \beta_2, \ldots, \beta_k]$ снова будет перестановкой.

◀ Примеры. 5. Пусть $M_1 = \{1, 2\}$, $M_2 = \{1, 2, 3\}$,

$$\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

— перестановка на множестве M_1,

$$\beta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \beta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

— перестановки на множестве M_2. Сплетение $[\alpha; \beta_1, \beta_2]$ перестановок β_1, β_2 с помощью α действует на множестве

$M_1 \times M_2$ так:

$$(1, 1)[\alpha;\ \beta_1,\ \beta_2] = ((1)\alpha,\ (1)\beta_1) = (2, 2),$$
$$(1, 2)[\alpha;\ \beta_1,\ \beta_2] = ((1)\alpha,\ (2)\beta_1) = (2, 1),$$
$$(1, 3)[\alpha;\ \beta_1,\ \beta_2] = ((1)\alpha,\ (3)\beta_1) = (2, 3),$$
$$(2, 1)[\alpha;\ \beta_1,\ \beta_2] = ((2)\alpha,\ (1)\beta_2) = (1, 3),$$
$$(2, 2)[\alpha;\ \beta_1,\ \beta_2] = ((2)\alpha,\ (2)\beta_2) = (1, 2),$$
$$(2, 3)[\alpha;\ \beta_1,\ \beta_2] = ((2)\alpha,\ (3)\beta_2) = (1, 1).$$

Таким образом, перестановка $[\alpha;\ \beta_1,\ \beta_2]$ имеет таблицу значений

$$\begin{pmatrix} (1, 1) & (1, 2) & (1, 3) & (2, 1) & (2, 2) & (2, 3) \\ (2, 2) & (2, 1) & (2, 3) & (1, 3) & (1, 2) & (1, 1) \end{pmatrix}.$$

При принятой нами нумерации множества $M_1 \times M_2$ ей сопоставляется следующая таблица:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}.$$

6. Пусть $\beta_1 = \beta_2 = \ldots = \beta_k = \beta$. Сплетение $[\alpha;\ \beta,\ \beta,\ \ldots,\ \beta]$ перестановок β с помощью перестановки α действует на произвольный элемент $(i, j) \in M_1 \times M_2$ согласно равенству

$$(i,\ j)[\alpha;\ \beta,\ \beta,\ \ldots,\ \beta] = ((i)\alpha,\ (j)\beta).$$

Это действие совпадает с действием прямого произведения перестановок α и β, т. е. имеет место равенство

$$[\alpha,\ \beta,\ \beta,\ \ldots,\ \beta] = \alpha \times \beta. \ \blacktriangleright$$

Пусть теперь G и H — произвольные множества перестановок на множествах M_1 и M_2 соответственно.

Определения. 1. *Суммой множеств перестановок G* и H (в предположении, что $M_1 \cap M_2 = \emptyset$) называется множество всевозможных перестановок вида $\alpha \oplus \beta$, где $\alpha \in G$, $\beta \in H$.

2. *Прямым произведением множеств перестановок G и H* называется множество всевозможных перестановок вида $\alpha \times \beta$, где $\alpha \in G$, $\beta \in H$.

3. *Сплетением множеств перестановок G и H* называется множество всевозможных перестановок вида $[\alpha;\ \beta_1, \beta_2, \ldots, \beta_k]$, где $k = |M_1|$, $\alpha \in G$, $\beta_1,\ \beta_2,\ \ldots,\ \beta_k \in H$.

Прямую сумму множеств перестановок G и M обозначим символом $G \oplus H$, их прямое произведение — символом $G \times H$, а сплетение — $G\,\imath\,H$. Понятно, что имеют место следующие равенства:

а) $|G \oplus H| = |G| \cdot |H|$;

б) $|G \times H| = |G| \cdot |H|$;

в) $|G \wr H| = |G| \cdot |H|^k$.

Теорема. *Если (G, M_1) и (H, M_2) — группы перестановок, то $G \oplus H$, $G \times H$ и $G \wr H$ также являются группами перестановок на соответствующих множествах.*

Доказательство. Достаточно убедиться, что произведение перестановок из одного из сконструированных множеств снова в нем содержится (см. упражнение 1 к § 8). Рассмотрим отдельно каждую из конструкций.

Пусть $\alpha \oplus \beta$, $\gamma \oplus \delta$ — две перестановки из $G \oplus H$. Произведение $(\alpha \oplus \beta) \cdot (\gamma \oplus \delta)$ этих перестановок действует на произвольный элемент $m \in M_1 \cup M_2$ так:

$$(m)\,((\alpha \oplus \beta) \cdot (\gamma \oplus \delta)) = ((m)\,(\alpha \oplus \beta))\,(\gamma \oplus \delta).$$

Но $(m)(\alpha \oplus \beta)$ совпадает либо с $(m)\alpha$ (при $m \in M_1$), либо с $(m)\beta$ (при $m \in M_2$). Если $m \in M_1$, то $(m)\alpha$ тоже содержится в M_1. Поэтому $((m)\alpha)(\gamma \oplus \delta) = ((m)\alpha)\gamma = (m)(\alpha \cdot \gamma)$. Аналогично, если $m \in M_2$, то $(m)\beta$ тоже содержится в этом множестве и $((m)\beta)(\gamma \oplus \delta) = ((m)\beta)\delta = (m)(\beta \cdot \delta)$. Итак, произведение $(\alpha \oplus \beta) \cdot (\gamma \oplus \delta)$ перестановок $\alpha \oplus \delta$ и $\gamma \oplus \delta$ множества $M_1 \cup M_2$ действует на произвольный элемент $m \in M_1 \cup M_2$ таким же образом, как и перестановка $(\alpha \cdot \gamma) \oplus (\beta \cdot \delta)$. Следовательно, имеет место равенство $(\alpha \oplus \beta) \cdot (\gamma \oplus \delta) = (\alpha \cdot \gamma) \oplus (\beta \cdot \delta)$. Поскольку G и H — группы, то $\alpha \cdot \gamma \in G$, $\beta \cdot \delta \in H$, т. е. $(\alpha \oplus \delta) \cdot (\gamma \oplus \delta) \in G \oplus H$ и $G \oplus H$ замкнуто относительно умножения перестановок.

Пусть теперь $\alpha \times \beta$, $\gamma \times \delta$ — две перестановки из $G \times H$. Произведение $(\alpha \times \beta) \cdot (\gamma \times \delta)$ действует на произвольную пару $(i, j) \in M_1 \times M_2$ согласно равенствам

$$(i, j)\,((\alpha \times \beta) \cdot (\gamma \times \delta)) = ((i)\alpha, (j)\beta)\,(\gamma \times \delta) = (((i)\alpha)\gamma, ((j)\beta)\delta),$$

т. е. на первую компоненту пары действует перестановка $\alpha \cdot \gamma$, а на вторую $\beta \cdot \delta$. Поскольку пара $(i, j) \in M_1 \times M_2$ произвольная, то это означает, что имеет место равенство

$$(\alpha \times \beta) \cdot (\gamma \times \delta) = (\alpha \cdot \gamma, \beta \cdot \delta).$$

Снова $\alpha \cdot \gamma \in G$, $\beta \cdot \delta \in H$, т. е. $G \times H$ замкнуто относительно умножения перестановок.

И наконец, пусть $A = [\alpha; \beta_1, \beta_2, \ldots, \beta_k]$, $B = [\gamma; \delta_1, \delta_2, \ldots, \delta_k]$ — две перестановки из $G \wr H$, причем

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & k \\ r_1 & r_2 & \ldots & r_k \end{pmatrix}.$$

Рассмотрим действие произведения $A \cdot B$ этих перестановок на произвольную пару $(i, j) \in M_1 \times M_2$. Имеем

равенства

$$(i, j)(A \cdot B) = ((i, j)A)B = ((i, j)[\alpha;\ \beta_1,\ \beta_2,\ \ldots,\ \beta_k])B =$$
$$= ((i)\alpha,\ (j)\beta_i)B = (r_i,\ (j)\beta_i)[\gamma;\ \delta_1,\ \delta_2,\ \ldots,\ \delta_k] =$$
$$= ((r_i)\gamma,\ (j)\beta_i\delta_{r_i}).$$

Таким образом, произведение $A \cdot B$ на первую компоненту пары (i, j) действует, как перестановка $\alpha \cdot \beta$, а на вторую компоненту — как перестановка $\beta_i \cdot \delta_{r_i} = \beta_i \cdot \delta_{(i)\alpha}$, т. е. $A \cdot B$ является сплетением перестановок $\beta_1 \cdot \delta_{r_1}, \beta_2 \cdot \delta_{r_2}, \ldots, \beta_k \cdot \delta_{r_k}$ с помощью перестановки $\alpha \cdot \beta$, а следовательно, содержится в $G \wr H$. Итак, $G \wr H$ замкнуто относительно умножения перестановок. Теорема доказана.

Конструкции прямой суммы, прямого произведения и сплетения групп перестановок позволяют по данным группам конструировать новые группы, т. е. существенно обогащают теорию новыми примерами. Оказывается, что многие из естественно возникающих групп перестановок можно построить из более простых с помощью рассмотренных в этом параграфе конструкций, а это оказывает существенную помощь при изучении таких групп перестановок.

Упражнения

1. Доказать, что прямая сумма перестановок — ассоциативная операция, т. е. для произвольных трех перестановок α, β, γ соответственно над множествами M_1, M_2, M_3, которые попарно не пересекаются, имеет место равенство

$$(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma).$$

2. Пусть $\langle k_1, k_2, \ldots, k_s\rangle$ — тип перестановки α на множестве M, $\langle l_1, l_2, \ldots, l_t\rangle$ — тип перестановки β на множестве M_2, и $M_1 \cap M_2 = \varnothing$. Каков тип перестановки $\alpha \oplus \beta$ на множестве $M_1 \cup M_2$?

3. Установите, что для порядков перестановок α, β, $\alpha \oplus \beta$ выполняется соотношение

$$\text{пор.}\ (\alpha \oplus \beta) = НОК\ \ (\text{пор.}\ \alpha,\ \text{пор.}\ \beta).$$

4. Постройте таблицу перестановки $\alpha \times \beta$, где

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

и таблицу, соответствующую $\alpha \times \beta$ при принятой нумерации множества $\{1, 2, 3\} \times \{1, 2, 3\}$.

5. Как, зная порядок перестановок α, β, определить порядок перестановки $\alpha \times \beta$?

6. Проверить, что группа перестановок

$$K = \{\varepsilon,\ \ (1, 2),\ \ (3, 4),\ \ (1, 2) \cdot (3, 4)\}$$

есть прямая сумма циклических групп второго порядка на множествах $\{1, 2\}$ и $\{3, 4\}$, а группа перестановок

$$L=\{\varepsilon,\ (1, 2)\circ(3, 4),\ (1, 3)\circ(2, 4),\ (1, 4)\circ(2, 3)\}$$

является прямым произведением циклической группы второго порядка над множеством $M=\{1, 2\}$ на себя, причем подстановки из этого прямого произведения записаны с учетом принятой нами нумерации элементов множества $M\times M$.

7. Указать обратные к перестановкам $\alpha\oplus\beta$, $\alpha\times\beta$, где α, β — перестановки на некоторых множествах.

8. Пусть

$$\alpha=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad \beta_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \beta_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \beta_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Построить перестановки $[\alpha;\ \beta_1,\ \beta_2,\ \beta_3]$, $[\alpha;\ \beta_2,\ \beta_1,\ \beta_3]$, $[\alpha;\ \beta_3,\ \beta_2,\ \beta_1]$. Совпадают ли они? Построить таблицы этих перестановок, записанные с учетом принятой нумерации элементов множества $\{1, 2, 3\}\times\{1, 2, 3\}$.

9. Как определить обратную к перестановке вида $[\alpha;\ \beta_1,\ \beta_2,\ \ldots,\ \beta_k]$?

10. Доказать, что сплетение двух циклических групп второго порядка совпадает с группой симметрий квадрата, при соответствующих обозначениях его вершин.

11. Пусть $f(x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6)=x_1x_2x_3+x_4x_5x_6$. Укажите конструкцию, с помощью которой группа симметрий этого многочлена строится из симметрических групп S_2, S_3, действующих на подходящих множествах.

12. Перестановка α над множеством M имеет следующее разложение в произведение взаимно простых циклов:

$$\alpha=(a_{11},\ a_{12},\ \ldots,\ a_{1k_1})\circ(a_{21},\ a_{22},\ \ldots,\ a_{2k_2})\circ\ldots\circ(a_{l1},\ a_{l2},\ \ldots,\ a_{lk_l}).$$

Докажите, что множество всех перестановок, которые коммутируют с α, совпадает с прямой суммой циклических групп C_{k_1}, C_{k_2}, ..., C_{k_l}, действующих на множествах

$$\{a_{11},\ a_{12},\ \ldots,\ a_{1k_1}\},\ \{a_{21},\ a_{22},\ \ldots,\ a_{2k_2}\},\ \ldots,\ \{a_{l1},\ a_{l2},\ \ldots,\ a_{lk_l}\}$$

соответственно.

§ 20. ВЕНГЕРСКИЙ ШАРНИРНЫЙ КУБИК

В 1975 г. венгерский архитектор профессор Э. Рубик создал математическую головоломку, которая получила в последующие годы широкое распространение во всем мире и является сейчас, пожалуй, наиболее популярной математической игрой. Математический анализ этой игры гораздо сложнее, чем анализ игры «в пятнадцать», вопросы и задачи, которые можно ставить в связи с ней, куда более разнообразны, хотя с точки зрения теории групп перестановок это игры одного типа.

1. Опишем вкратце головоломку Э. Рубика. Она представляет собой пластмассовый куб, разбитый на 27 одинаковых кубиков плоскостями, параллельными граням куба; 26 кубиков являются наружными, а один — внутренний. Внутренний кубик удален, а наружные кубики, на которых изнутри имеются специальные выступы, с помощью крестовины сцеплены так, что любая из плит, образованных девятью кубиками, грани которых параллельны некоторой грани куба, может свободно вращаться вокруг центра в любом направлении. При повороте одной из плит на углы 90°, 180° или 270° свобода вращений системы полностью сохраняется: любую из плит снова можно вращать вокруг центра в любую сторону. Внешние грани каждого из 26 маленьких кубиков окрашены в шесть разных цветов: красный, оранжевый, желтый, зеленый, синий, белый (по 9 граней каждого цвета).

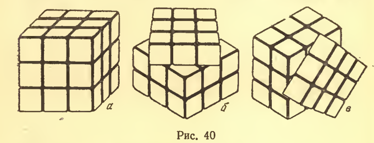


Рис. 40

Общий вид куба изображен на рис. 40 *а*, на рис. 40 *б*, *в* указаны возможные повороты плит — внешних и внутренней. В начальном положении маленькие кубики расположены так, что все грани большого куба окрашены в один цвет. Затем с помощью нескольких последовательных вращений грани куба приобретают пеструю окраску. Цель игры состоит в том, чтобы, получив в руки такой пестро окрашенный кубик, с помощью поворотов плит перейти к начальной раскраске, т. е. добиться такой расстановки кубиков, при которой все грани большого куба окрашены в один цвет.

Эта головоломка получила название «венгерский шарнирный кубик» или «кубик Рубика». Исследованию задач, с ней связанных, посвящено большое число научно-популярных статей, опубликованных в разных странах, и даже несколько книг (например, книга В. Хинце «Венгерский волшебный кубик» на немецком языке, вышедшая в 1982 г. в берлинском издательстве «VEB Deutscher Verlag der Wiss-

enschaften»). Из публикаций в отечественных журналах отметим статьи И. Константинова «Венгерский кубик» («Наука и жизнь», 1981, № 3; 1982, № 2), В. Залгаллера, С. Залгаллера «Венгерский шарнирный кубик» («Квант», 1980, № 12), М. Евграфова «Механика волшебного кубика» («Квант», 1982, № 2), В. Дубровского «Алгоритм волшебного кубика» («Квант», 1982, № 7), «Математика волшебного кубика» («Квант», 1982, № 8), «Кубик в картинках» («Квант», 1983, № 9), Ю. Демкова «Поворачиваем кубики» («Квант», 1981, № 12) и некоторые другие.

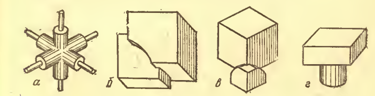


Рис. 41

Уже из названий некоторых из этих публикаций видно, какими вопросами интересуются при рассмотрении кубика Рубика. В первую очередь, хочется узнать, как же он устроен, каков механизм, позволяющий осуществлять такие вращения. Во-вторых, естественно возникает желание научиться переходить к начальной окраске кубика из любого возможного его «пестрого» состояния. Конечно, если «пестрая» раскраска получена из начальной с помощью ряда вращений плит, то перейти от такого состояния к начальному всегда можно. Поэтому хочется иметь набор правил — *алгоритм*, который обеспечит достижение начального состояния из любого возможного. Для выработки такого алгоритма строят математическую модель решаемой задачи. В этой-то модели и возникает группа перестановок, связанная с кубиком Рубика. Вспомогательные задачи, которые необходимо решить, — это научиться строить системы образующих возникающей группы перестановок и раскладывать ее элементы в произведение образующих элементов. Обе задачи упрощаются, если заметить, что группа перестановок, связанная с кубиком Рубика, строится из уже известных читателю групп с помощью рассмотренных в предыдущем параграфе конструкций.

Вначале рассмотрим, как устроен волшебный кубик. В нем 27 основных деталей: крестовина (рис. 41 *а*), 12 боковых кубиков (рис. 41 *б*), 8 угловых кубиков (рис. 41 *в*)

и 6 центральных кубиков (рис. 41 г). На самом деле, как видно из рис. 41, «кубики» — это совсем не кубики, а более сложные тела. В большой куб они сложены так, что извне кажутся кубиками. Кубики, расположенные в центре каждой из граней (поэтому мы их будем называть *центральными*), крепятся на крестовину. У них окрашена одна сторона (внешняя). Средние кубики, у которых раскрашены 2 внешние стороны, расположены в середине каждого ребра, а угловые кубики, у которых раскрашены 3 внешние грани, расположены в вершинах куба. Расположение кубиков в кубе хорошо видно на рис. 42, на котором куб изображен со снятыми передней плитой и одним средним кубиком. Внутренние выступы на средних и угловых кубиках сделаны так, что при составлении куба из этих выступов образуется почти цилиндрическое тело, а на среднем слое образуется кольцеобразное углубление. При повороте плиты цилиндрическое тело вращается в кольцеобразном углублении. Вот и весь механизм кубика Рубика, не считая мелких второстепенных деталей.

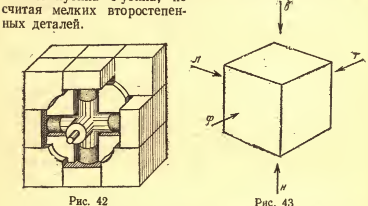


Рис. 42 Рис. 43

2. Остановимся теперь на описании алгоритма приведения кубика Рубика из «пестрого» состояния в начальное. Условимся вначале о следующих удобных сокращениях.

Поскольку при вращениях плит мы интересуемся лишь взаимным расположением маленьких кубиков в большом кубе, можно считать расположение куба в пространстве фиксированным, т. е. считать его крестовину жестко закрепленной, а центральные кубики — неподвижными. Это означает, что возможны лишь вращения шести внешних плит куба. Обозначим грани куба буквами (рис. 43)

«ф» (фасад), «т» (тыл), «в» (верх), «н» (низ), «л» (левая сторона), «п» (правая сторона). Маленькие кубики можно теперь определять наборами букв: центральным кубикам соответствует одна буква (например, кубику фасада — буква «ф»), средним кубикам — две буквы (например, кубику, принадлежащему фасадной и левой грани, — буквы «фл»), угловым кубикам — три буквы (например, кубику, принадлежащему фасадной, левой и верхней граням, — буквы «флв»).

Прописными буквами Ф, Т, В, Н, Л, П будем обозначать вращения соответствующей грани (плиты) на угол $\pi/2$ по часовой стрелке. Вращения против часовой стрелки обозначаются этими же буквами в степени -1. Это оправдано, поскольку каждое из вращений осуществляет некоторую перестановку множества маленьких кубиков с учетом раскраски и, следовательно, можно говорить об обратной перестановке. Понятно, что обратной к перестановке Ф будет перестановка $Ф^{-1}$, и аналогично для других типов вращений. Последовательностям вращений граней будут отвечать «слова», составленные из букв Ф, Т, В, Н, Л, П в степенях ± 1. Например, словом

$$ФТ^2Н^{-1}Л^{-3} = ФТТН^{-1}Л^{-1}Л^{-1}Л^{-1} \quad (1)$$

описывается следующая последовательность вращений:

а) фасадную грань повернуть на угол $\pi/2$ по часовой стрелке;

б) тыловую грань дважды повернуть на угол $\pi/2$, или, что то же самое, повернуть на угол π по часовой стрелке;

в) нижнюю грань повернуть на угол $\pi/2$ против часовой стрелки;

г) левую грань повернуть на угол $3\pi/2$ против часовой стрелки.

Каждому из этих вращений соответствует некоторая перестановка маленьких кубиков с учетом их раскраски, а всей последовательности — произведение таких перестановок. В результате выполнения серии вращений а) — г) маленькие кубики «пропутешествуют» и займут новые места в кубе.

Будем называть расположения кубиков внутри большого куба его *состояниями*. Если от состояния S к состоянию S' можно перейти серией вращений σ, то будем записывать это так: $S' = (S)\sigma$. Различные серии вращений могут переводить куб, вообще говоря, в одно и то же

состояние. Например, имеем для любого состояния S:

$$(S)\text{Ф}^2=(S)\text{Ф}^{-2},\quad (S)\text{Т}=(S)\text{Т}^{-3},\quad (S)\text{Н}^3=(S)\text{Н}^{-1},$$
$$(S)\text{П}^4=S,\quad (S)\text{Л}\cdot\text{Л}^{-1}=S.$$

Читатель без труда продолжит этот список.

Состояние куба назовем *допустимым*, если его можно получить из начального вращениями граней куба. Понятно, что из любого допустимого состояния можно перейти к начальному — для этого нужно просто обратить последовательность вращений. Например, если состояние куба S получено из начального состояния S_0 в результате серии вращений (1), то, применяя к кубу в состоянии S последовательность вращений

$$\text{ЛЛЛНТ}^{-1}\text{Т}^{-1}\text{Ф}^{-1}=\text{Л}^3\text{НТ}^{-2}\text{Ф}^{-1},$$

перейдем к состоянию S_0, т. е. $(S)\text{Л}^3\text{НТ}^{-2}\text{Ф}^{-1}=S_0$.

Опишем теперь один из возможных алгоритмов сборки кубика Рубика, т. е. укажем правила, руководствуясь которыми от любого допустимого состояния можно перейти к начальному. В большинстве алгоритмов вращения граней, осуществляемые при сборке кубика Рубика, группируются в стандартные комбинации из двух вращений X, Y ($X, Y\in\{\text{Ф, П, Л, В, Н, Т}\}$):

а) комбинация $X^{-1}YX$ — *сопряжение вращения Y с помощью вращения X*;

б) комбинация $X^{-1}Y^{-1}XY$ — *коммутатор вращений X, Y.*

Можно рассматривать также сопряжения и коммутаторы степеней основных вращений, например:

а) $\text{Ф}^{-2}\text{В}^3\text{Ф}^2=\text{Ф}^2\text{В}^3\text{Ф}^2$ — сопряжение вращения В^3 с помощью вращения $\text{Ф}^2=\text{Ф}^{-2}$;

б) $\text{П}^2\text{В}^2\text{П}^{-2}\text{В}^{-2}=\text{П}^2\text{В}^2\text{П}^2\text{В}^2$ — коммутатор вращений $\text{П}^{-2}(=\text{П}^2)$, $\text{В}^{-2}(=\text{В}^2)$.

Легко проверяется, что коммутатор основных вращений прилегающих граней переставляет три средних кубика циклически. Например, коммутатор $\text{П}^{-1}\text{Ф}^{-1}\text{ПФ}$ действует на кубики, стоящие на местах фн, фп, пв следующим образом (рис. 44):

$$\text{фн}\to\text{пв}\to\text{фп}\ (\to\text{фн}).$$

При этом некоторые кубики остаются неподвижными, а угловые также перемещаются.

Процесс сборки кубика Рубика осуществляется в 4 этапа. К выполнению следующего этапа нужно приступать лишь тогда, когда предыдущий этап полностью закончен. При

описании этапов сборки буквами x, y, z будем обозначать какие-то из граней куба, имеющие общую вершину, а символами X, Y, Z — основные вращения граней x, y, z соответственно.

Этап 1. Расстановка на своих местах средних кубиков. Серия вращений

$$X^{-1}Z^{-1}Y^{-1}X^{-1}YXZ \qquad (2)$$

граней куба x, y, z переставляет два средних кубика, принадлежащие грани x, и оставляет неподвижными остальные средние кубики. Применяя эту серию к некоторому состоянию S куба, получим новое состояние S', отличающееся от S расположением угловых и двух средних кубиков. Например, для серии $Ф^{-1}В^{-1}П^{-1}Ф^{-1}ПФВ$ имеем (рис. 45)

$$фл \to фв, \qquad фв \to фл.$$

Серии вращения вида (2) позволяют переставить любые два из средних кубиков. Для этого нужно с помощью вспомогательных ходов поставить переставляемые кубики на соответствующие места в одной из граней куба, применить серию вращений (2) и, выполняя обратную последовательность ходов, перейти к требуемому состоянию.

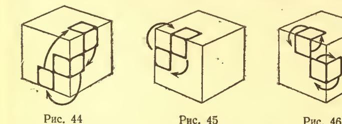


Рис. 44 Рис. 45 Рис. 46

Этап 1 закончен, если все средние кубики расположены на своих местах. Однако при этом они могут оказаться неправильно ориентированными (цвет среднего кубика грани не соответствует цвету ее центрального кубика).

Этап 2. Правильная ориентация средних кубиков, стоящих на своих местах. Произведение трех коммутаторов

$$(XY^{-1}X^{-1}Y)\,(YZ^{-1}Y^{-1}Z)\,(ZX^{-1}Z^{-1}X) \qquad (3)$$

одновременно поворачивает на своих местах два из кубиков, принадлежащих грани x, не меняя при этом рас-

положения других средних кубиков. Например, серия

$$(Ф П^{-1} Ф^{-1} П)(П В^{-1} П^{-1} В)(В Ф^{-1} В^{-1} Ф)$$

поворачивает на своих местах средние кубики фв и фп (рис. 46). Последовательности вращений вида (3), выполненные для подходящих граней, позволяют одновременно менять ориентацию любых двух из средних кубиков (почему?). Выполняя совместную переориентацию пар средних кубиков, можно все их расположить на своих местах так, как они располагаются в начальном состоянии куба. Это следует из того, что состояние, в котором все средние кубики, кроме одного, правильно расположены на своих местах, не может быть допустимым.

Рис. 47

Рис. 48

Этап 3. Расстановка на своих местах угловых кубиков. Степень

$$(XYX^{-1}Y^{-1})^3 \qquad (4)$$

коммутатора вращений X, Y соседних граней x, y осуществляет одновременную перестановку пар угловых кубиков, которые принадлежат граням, имеющим с x, y два общих ребра. Например (рис. 47), третья степень коммутатора $ФПФ^{-1}П^{-1}$ переставляет угловые кубики так:

$$\begin{cases} фвл \to фвп, \\ фвп \to фвл, \end{cases} \qquad \begin{cases} пнф \to пнт, \\ пнт \to пнф. \end{cases}$$

Произведение степеней коммутаторов

$$(XZX^{-1}Z^{-1})^3 (Y^{-1}X^{-1}YX)^3 \qquad (5)$$

осуществляет перестановку трех угловых кубиков, принадлежащих грани x. Например, серия вращений

$$(ФВФ^{-1}В^{-1})^3 (П^{-1}Ф^{-1}ПФ)^3$$

перемещает угловые кубики фасадной грани следующим образом:

$$фнл \to фвл \to фнп \to фнл.$$

После выполнения каждой из серий поворотов (4), (5) средние кубики не меняют своего положения; остаются на своих местах также угловые кубики, которые не учитывались при рассмотрении серии.

С помощью последовательностей вращений вида (4), (5) все угловые кубики можно расставить по своим местам (проверьте!). При этом надо учитывать, что в допустимом состоянии не может случиться так, чтобы все средние кубики были расположены как в начальном состоянии, а все угловые, кроме двух, стояли на своих местах: если не все угловые кубики стоят на своих местах, то их не меньше чем 3.

Этап 4. Переориентация угловых кубиков, стоящих на своих местах. Последовательность вращений

$$\sigma=[(X^{-1}ZXZ^{-1})(Z^{-1}YZY^{-1})(Y^{-1}XYX^{-1})]^2 \qquad (6)$$

одновременно поворачивает каждый из трех угловых кубиков, принадлежащих грани x, вокруг соответствующей диагонали куба на угол $2\pi/3$ по часовой стрелке. А последовательность вращений σ^{-1} поворачивает эти кубики вокруг тех же осей на угол $4\pi/3$ по часовой стрелке. Например, вращения σ, составленные для граней ф, в, п, поворачивают угловые кубики фвл, фвп, фнп (рис. 48). При этом расположение и ориентация других кубиков не изменяются. Понятно, что с помощью последовательностей вращений σ и σ^{-1} можно переориентировать любые 3 угловых кубика. Если учесть, что в допустимом состоянии не может случиться так, чтобы все средние кубики были расположены как в начальном состоянии, все угловые кубики были на своих местах и лишь один из них был бы неправильно повернут, то закончить этап 4, а следовательно, и сборку кубика в целом не составляет труда.

Описанный здесь алгоритм — далеко не самый экономный. Сборка кубика с его помощью может быть весьма длительным процессом, требующим большого числа ходов. Существуют более экономные алгоритмы, в частности, описанные в отмеченных выше статьях. Однако приведенный алгоритм поможет нам построить математическую теорию игры, после чего читатель сам сможет разрабатывать такие алгоритмы.

3. Опишем группу перестановок, которая «управляет» состояниями кубика Рубика. Полностью описать состояние куба можно, указав место, которое занимает каждый маленький кубик в нем и, ориентацию кубика на этом месте. Средние кубики могут быть ориентированы на каждом месте двумя способами, а угловые — тремя. Пусть кубик Рубика находится в начальном состоянии. Зануме-

руем его угловые кубики в каком-либо порядке числами 1, 2, ..., 8, а средние числами 9, 10, ..., 20. Этими же числами занумеруем места, на которых стоят маленькие кубики. Любое состояние куба после этого можно характеризовать перестановкой, указывающей номера угловых и средних кубиков, стоящих при этом состоянии на местах 1—20. Если в состоянии S на месте с номером i стоит кубик с номером j_i ($1 \leqslant i \leqslant 20$), то этому состоянию однозначно ставится в соответствие перестановка

$$\varphi_S = \begin{pmatrix} 1 & 2 & 3 & \dots & 20 \\ j_1 & j_2 & j_3 & \dots & j_{20} \end{pmatrix}.$$

Перестановка φ_S определяет только места, занимаемые маленькими кубиками, состояние S ею однозначно не определяется — нужно определить еще ориентацию кубиков. Для задания ориентации угловых кубиков фиксируем две противоположные грани куба — например, верхнюю и нижнюю. Предположим, что эти грани окрашены в красный (верхняя) и желтый (нижняя) цвета. Любой угловой кубик имеет либо красную, либо желтую грань. Угол, на который нужно повернуть угловой кубик вокруг вершины куба, чтобы эта его грань заняла положение вверху (красная) либо внизу (желтая), и определяет ориентацию углового кубика. Этот угол может равняться 0, $2\pi/3$, $4\pi/3$. Условимся обозначать ориентацию углового кубика, соответствующую повороту на 0, символом «0», повороту на $2\pi/3$ — символом «1», а повороту на $4\pi/3$ — символом «2». После этого при любом состоянии куба расположение углового кубика с учетом его ориентации описывается парой чисел (i, s), $1 \leqslant i \leqslant 8$, $0 \leqslant s \leqslant 2$, где i — номер места, на котором он стоит, s — его ориентация. При передвижениях кубика эта пара изменяется — как первая координата, так и вторая. Для того чтобы указать ориентацию среднего кубика, на каждом ребре куба фиксируем направление (укажем стрелку) и «нарисуем» такое же направление на среднем кубике так, чтобы в начальном состоянии оба направления совпадали. После этого при любом состоянии куба положение среднего кубика с учетом его ориентации описывается парой чисел (j, t), $9 \leqslant j \leqslant 20$, $t = 0, 1$, где j — номер места, на котором стоит кубик, а $t = 0$, если ориентации кубика и ребра, на котором он расположен, совпадают, и $t = 1$, если они противоположны. Таким образом, состояния куба однозначно характеризуются перестановками

множества

$$K=\{1, 2, \ldots, 8\}\times\{0, 1, 2\}\cup\{9, 10, \ldots, 20\}\times\{0, 1\}.$$

Каковы же эти перестановки?

Поскольку при вращениях граней средние кубики могут передвигаться только на место средних, а угловые — на место угловых, то любая перестановка α_S множества K, задающая некоторое состояние куба S, определяет некоторую перестановку $\alpha_S^{(1)}$ из множества $\{1, 2, \ldots, 8\}\times\{0, 1, 2\}$ — перестановку угловых кубиков с учетом ориентации — и некоторую перестановку $\alpha_S^{(2)}$ из множества $\{9, 10, \ldots, 20\}\times\{0, 1\}$ — перестановку средних кубиков с учетом ориентации. Эти перестановки действуют на непересекающихся множествах, объединение которых совпадает с K. Поэтому, согласно определению прямой суммы перестановок, получаем

$$\alpha_S=\alpha_S^{(1)}\oplus\alpha_S^{(2)}.$$

Посмотрим теперь, как же устроены перестановки множеств угловых и средних кубиков с учетом ориентации. Задать перестановку $\alpha_S^{(1)}$ означает указать место каждого из угловых кубиков (чему соответствует перестановка $\varphi_S^{(1)}$ множества $\{1, 2, \ldots, 8\}$, являющаяся ограничением перестановки φ_S на это множество) и указать ориентацию каждого из угловых кубиков (чему будет соответствовать задание для каждого из кубиков «своей» перестановки на множестве $\{0, 1, 2\}$, которая является степенью цикла длины 3). Итак, перестановке $\alpha_S^{(1)}$ сопоставляется набор $[\varphi_S^{(1)}; \tau_1, \tau_2, \ldots, \tau_8]$, где τ_i определяет ориентацию i-го кубика ($1\leqslant i\leqslant 8$). Иными словами, перестановка $\alpha_S^{(1)}$ является сплетением перестановок $\tau_1, \tau_2, \ldots, \tau_8$ множества $\{0, 1, 2\}$, содержащихся в циклической группе C_3 этого множества, с помощью некоторой перестановки из симметрической группы S_8.

Аналогично, задать перестановку $\alpha_S^{(2)}$ означает указать место каждого среднего кубика (чему соответствует ограничение $\varphi_S^{(2)}$ перестановки φ_S на множество $\{9, 10, \ldots, 20\}$) и его ориентацию (чему соответствует задание для каждого из кубиков «своей» перестановки τ_i на множестве $\{0, 1\}$). Это означает, что перестановка $\alpha_S^{(2)}$ является сплетением перестановок $\tau_9, \tau_{10}, \ldots, \tau_{20}$ множества $\{0, 1\}$ с помощью некоторой перестановки из симметрической группы S_{12}, действующей на множестве $\{9, 10, \ldots, 20\}$.

Таким образом, можно сказать, что любое состояние кубика Рубика однозначно описывается перестановкой

множества K, имеющей вид

$$[\varphi^{(1)};\ \tau_1,\ \tau_2,\ \ldots,\ \tau_8] \oplus [\varphi^{(2)};\ \tau_9,\ \tau_{10},\ \ldots,\ \tau_{20}], \qquad (7)$$

где $\varphi^{(1)} \in S_8$, $\varphi^{(2)} \in S_{12}$ (S_{12} действует на множестве $\{9, 10, \ldots, 20\}$), $\tau_i \in C_3$ при $i = 1, 2, \ldots, 8$ и $\tau_i \in S_2$ при $i = 9, 10, \ldots, 20$. А множеству всех состояний соответствует группа перестановок

$$H = (S_8 \wr C_3) \oplus (S_{12} \wr S_2),$$

действующая на множестве K. Отсюда сразу получаем, что общее число состояний кубика Рубика равно $(8! \cdot 3^8)(12! \cdot 2^{12})$.

Опишем теперь перестановки, которыми задаются допустимые состояния волшебиого кубика. Оии, очевидно, будут образовывать группу, поскольку произведение перестаиовок, отвечающих допустимым состояниям, тоже задает иекоторое допустимое состояние (почему?). Покажем, что эта группа состоит из тех перестановок группы H вида (7), для которых выполняются следующие три условия:

а) $\varphi^{(1)} \oplus \varphi^{(2)}$ — четная перестановка;

б) $\tau_1 \circ \tau_2 \circ \ldots \circ \tau_8 = \varepsilon$ — тождественная перестановка множества $\{0, 1, 2\}$;

в) $\tau_9 \circ \tau_{10} \circ \ldots \circ \tau_{20} = \varepsilon$ — тождественная перестановка миожества $\{0, 1\}$.

Проверим сначала, что условия а), б), в) необходимы. Вращеиие любой из граией на угол $\pi/2$ определяет циклическую перестановку иа множествах угловых и средних кубиков этой грани. Пусть при таком вращеиии куб переходит из состояния S в состояиие S'. Если состояние S описывается перестановкой

$$[\varphi_S^{(1)};\ \tau_1,\ \ldots,\ \tau_8] \oplus [\varphi_S^{(2)};\ \tau_9,\ \ldots,\ \tau_{20}],$$

а состояние S' — перестаиовкой

$$[\varphi_{S'}^{(1)};\ \sigma_1,\ \ldots,\ \sigma_8] \oplus [\varphi_{S'}^{(2)};\ \sigma_9,\ \ldots,\ \sigma_{20}],$$

то $\varphi_{S'}^{(1)} = \varphi_S^{(1)} \circ \pi$, $\varphi_{S'}^{(2)} = \varphi_S^{(2)} \circ \pi$, где π — циклические перестановки множеств угловых и средиих кубиков этой граии. Это циклы длины 4, т. е. иечетиые перестаиовки. Поэтому перестаиовки $\varphi_S^{(1)}$ и $\varphi_{S'}^{(1)}$, $\varphi_S^{(2)}$ и $\varphi_{S'}^{(2)}$ имеют соответствеино противополо́жиые четности. Следовательио, четности перестановок $\varphi_S^{(1)} \oplus \varphi_S^{(2)}$ и $\varphi_{S'}^{(1)} \oplus \varphi_{S'}^{(2)}$ совпадают. Если состояиие S — допустимое, то от него можно перейти к иачальному состоянию с помощью серии вращеиий граней. На каждом шаге при этом будет появляться новое состоя-

ние S', четность подстановки $\varphi_{S'}^{(1)} \oplus \varphi_{S'}^{(2)}$ для которого совпадает с четностью $\varphi_{S}^{(1)} \oplus \varphi_{S}^{(2)}$. Поэтому четность подстановки $\varphi_{S}^{(1)} \oplus \varphi_{S}^{(2)}$ для допустимого состояния S совпадает с четностью такой подстановки для начального состояния, а ему соответствует четная подстановка. Итак, условие а) необходимо.

Далее, легко проверяется, что перестановки, определяющие ориентацию угловых кубиков, не изменяются при произвольных вращениях верхней и нижней граней куба и при вращениях остальных граней на угол π. При вращениях одной из граней ф, п, л, т на углы $\pi/2$, $3\pi/2$ две перестановки, задающие ориентацию кубиков противоположных вершин, умножаются на цикл $(0, 1, 2)$, а две другие — на цикл $(0, 1, 2)^2 = (0, 1, 2)^{-1}$. Следовательно, произведение всех таких перестановок $\tau_1, \tau_2, \ldots, \tau_8$ для каждого допустимого состояния такое же, как и для начального, для которого оно, очевидно, равно ε.

Перестановки, определяющие ориентацию средних кубиков, либо не изменяются при поворотах грани, либо все изменяются на противоположные (т. е. умножаются на транспозицию $(0, 1)$). Поэтому их произведение остается прежним, т. е. выполняется условие в).

Описывая алгоритм сборки кубика, мы использовали три совсем неочевидных утверждения:

1) состояние, в котором все средние кубики, кроме одного, правильно расположены на своих местах, не может быть допустимым;

2) состояние, в котором все средние кубики правильно расположены на своих местах и все угловые, кроме двух, стоят на своих местах, не может быть допустимым;

3) состояние, в котором все средние кубики правильно расположены на своих местах, все угловые — тоже, но один из них неправильно повернут, не может быть допустимым.

Правильность утверждений 1) — 3) следует из необходимости условий а) — в) для того, чтобы перестановка множества K определяла допустимое состояние кубика. Действительно, для состояний кубика Рубика, не удовлетворяющих требованию 1), очевидно, не выполняется условие б), а для состояний, не удовлетворяющих требованию 3), — условие в). Состояние S, не удовлетворяющее условию 2), не может быть допустимым, поскольку соответствующая ему подстановка $\varphi_{S}^{(1)} \oplus \varphi_{S}^{(2)}$ — нечетная. В самом деле, так как все средние кубики стоят на своих местах, то $\varphi_{S}^{(2)}$ — тождественная подстановка, а $\varphi_{S}^{(1)}$ — транс-

позиция. Поэтому $\varphi_S^{(1)} \oplus \varphi_S^{(2)}$ — нечетная, как прямая сумма нечетной подстановки с четной.

Убедимся теперь, что условия а) — в) являются также и достаточными. Пусть S — некоторое состояние кубика Рубика, которое характеризуется перестановкой из группы H, удовлетворяющей условиям а) — в). Применим к этому состоянию описанный нами алгоритм сборки кубика. Первый этап алгоритма выполняется беспрепятственно, поскольку его можно применить к любому состоянию и получить нужный результат. Второй этап алгоритма можно провести всегда, если состояние S удовлетворяет условию 1). Но это так и есть, поскольку условие 1) — следствие условия б). После осуществления второго этапа все средние кубики правильно расположены на своих местах и полученному состоянию куба отвечает перестановка множества K вида

$$[\varphi_S^{(1)};\ \tau_1,\ \tau_2,\ \ldots,\ \tau_8] \oplus \varepsilon^{(2)},$$

где $\varepsilon^{(2)}$ — тождественная перестановка множества $\{9,\ 10,\ \ldots,\ 20\} \times \{0,\ 1\}$. Отсюда следует, что перестановка $\varphi_S^{(1)}$ — четная. А четную перестановку можно либо разложить в произведение циклов длины 3 (см. упражнение 7 к § 15), либо разбить на произведение пар транспозиций. Поэтому можно осуществить третий этап сборки волшебного кубика. Заметим, что описывая ранее этот и следующий этап, мы намеренно опустили некоторые подробности; теперь читатель легко их восполнит.

После третьего этапа сборки состояние куба будет характеризоваться перестановкой множества K вида

$$[\varepsilon^{(1)};\ \tau_1,\ \tau_2,\ \ldots,\ \tau_8] \oplus \varepsilon^{(2)},$$

где $\varepsilon^{(1)}$ — тождественная перестановка множества $\{1,\ 2,\ \ldots,\ 8\}$, а τ_i — циклические или тождественная перестановка множества $\{0,\ 1,\ 2\}$, причем $\tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_8 = \varepsilon$. Последнее равенство, как было сказано, означает, что это состояние удовлетворяет условию 3), т. е. к этому состоянию можно применить четвертый этап сборки кубика.

Таким образом, группа перестановок G множества K, характеризующая допустимые состояния кубика, является собственной подгруппой группы H. Для любой перестановки из H вида (7) может быть выполнено одно из следующих условий:

а) $\varphi^{(1)} \oplus \varphi^{(2)}$ — либо четная, либо нечетная (2 возможности);

б) перестановка $\tau_1 \circ \tau_2 \circ \ldots \circ \tau_8$ равна либо ε, либо (0, 1, 2), либо (0, 2, 1) (3 возможности);

в) перестановка $\tau_9 \circ \tau_{10} \circ \ldots \circ \tau_{20}$ равна либо ε, либо (1, 0) (2 возможности).

Всего можно составить 12 комбинаций этих возможностей, т. е. перестановка из H вида (7) может удовлетворять одному из 12 наборов условий. Этими условиями как раз описываются классы смежности группы G по подгруппе H (почему?), т. е. G — подгруппа индекса 12 в H.

После всего сказанного становится понятно, как формулировать задачи, связанные с кубиком Рубика на языке теории групп перестановок:

В группе G фиксирована система образующих перестановок, которые соответствуют вращениям граней кубика Рубика. Требуется указать алгоритм, руководствуясь которым любую перестановку можно было бы разложить в произведение образующих.

При этом важна оценка длины разложения, а она может существенно зависеть от выбранного алгоритма (из предыдущих примеров уже известно, что разложение подстановки в произведение образующих не однозначно).

По мере исследования свойств группы G такие оценки существенно понижались. В соответствии с одним из первых алгоритмов любую перестановку из группы G можно было бы разложить в произведение не более чем 277 образующих из указанной системы, т. е. «пестрый» кубик можно было бы перевести в начальное состояние не более чем за 277 поворотов граней. После более детального анализа был разработан алгоритм, позволяющий раскладывать перестановки из G в произведение образующих длины не более 52, причем высказано мнение, что можно ограничиться произведениями длины не более 23.

На самом деле оценку длины возможных разложений можно исследовать независимо, без рассмотрения алгоритмов, позволяющих такое разложение осуществлять

Упражнения

1. Как действуют на угловые кубики серии вращений а) $(\Phi^2\Pi^2)^3$, б) $(\Phi\Pi\Phi^{-1}\Pi^{-1})^3$, в) $\Phi H^2\Phi^{-1}H^{-1}$, г) $Л^{-1}В^{-1}\Pi^{-1}ВЛВ^{-1}\Pi В$?

2. Каков порядок перестановок из группы G, определяемых сериями вращений $H^2\Pi^2$, $ВЛВ^{-1}Л^{-1}$?

3. Проверить, что серия вращений $В^{-1}Л\Pi^{-1}\Phi^2\Pi Л^{-1}В^{-1}$ осуществляет циклическую перестановку трех средних кубиков, расположенных на трех гранях «буквой Т».

4. Указать последовательность вращений граней куба, меняющую местами угловые кубики, расположенные по диагонали (с изменением ориентации).

5. Проверить, что последовательность вращений $П^2Н^{-1}Л^{-1}ПВ^2ЛП^{-1}Ф^2НП^2$ циклически переставляет средние кубики, принадлежащие одной грани, а все другие кубики оставляет на местах.

6. «Кубик без раскраски». Маленькие кубики в кубе занумерованы: угловые — числами 1, 2, ..., 8, а средние — числами 9, 10, ..., 20. Куб не раскрашен. Если пронумеровать места, которые первоначально занимают маленькие кубики, теми же числами, то любое состояние такого куба однозначно описывается некоторой перестановкой множества {1, 2, ..., 20}. Какие перестановки этого множества соответствуют допустимым состояниям куба?

7. Проверить, что любой цикл (i, j, k) длины 3 над некоторым множеством является коммутатором транспозиций над этим множеством.

8. Подгруппа некоторой группы G, порожденная всевозможными коммутаторами элементов из G, называется *коммутантом* G. Найти коммутант группы S_n.

9. Предположим, что волшебный кубик окрашен в 3 цвета так, что в начальном состоянии противоположные грани окрашены одинаково. Описать допустимые состояния такого кубика.

10. Кубик Рубика был разобран и заново сложен так, что в «начальном» состоянии ему отвечает перестановка вида (7), для которой $\varphi^{(1)} \oplus \varphi^{(2)}$ — нечетная,

$$\tau_1 \circ \tau_2 \circ \ldots \circ \tau_8 = (0, 1, 2), \quad \tau_9 \circ \tau_{10} \circ \ldots \circ \tau_{20} = (0, 1).$$

Можно ли от любого состояния с такими же свойствами перейти к «начальному»?

11. Докажите, что условия

$$\tau_1 \circ \tau_2 \circ \ldots \circ \tau_8 = e \quad \text{и} \quad \tau_9 \circ \tau_{10} \circ \ldots \circ \tau_{20} = e,$$

накладываемые на перестановки вида (7), характеризующие состояния кубика, не зависят от способа определения ориентации угловых и средних кубиков.

12. Алгоритм «послойной» сборки кубика Рубика состоит в следующем:

Этап 1. Устанавливаем на своих местах правильно ориентированные средние кубики нижней грани.

Этап 2. Устанавливаем на своих местах правильно ориентированные угловые кубики нижней грани.

Этап 3. Устанавливаем на свои места средние кубики серединной плиты (параллельной нижней грани).

Этап 4. Переориентируем средние кубики верхней грани: средние кубики установим так, чтобы цвет их верхней грани совпал с цветом центрального кубика верхней грани.

Этап 5. Переставляем верхние реберные кубики.

Этап 6. Переориентируем верхние угловые кубики.

Этап 7. Переставляем верхние угловые кубики.

Попробуйте разработать этот алгоритм подробно и дать его детальное описание.

§ 21. ДРУГИЕ ИГРЫ

Кроме игры в «пятнадцать» и кубика Рубика известны и другие занимательные головоломки, математический анализ которых приводит к рассмотрению перестановок

и групп перестановок. Некоторые из них указаны в упражнениях к § 18 как обобщение игры «в пятнадцать». Приведем краткое описание нескольких типов игр без подробного рассмотрения их математической теории. Пользуясь рассмотренными здесь образцами, читатель сам сможет дать полный анализ той или иной игры.

1. Игры типа игры «хамелеон». Игра «хамелеон», описанная в упражнении 7 к § 18, совпадает с игрой в «восемь» (упражнение 9 к § 18). Однако первоначальная формулировка этой игры допускает различные обобщения, которые можно условно назвать перестановочными играми на графах. Опишем такую игру в общем случае (рис. 49).

Пусть имеется некоторый неориентированный граф, вершины которого обозначены кружочками и занумерованы. Предположим, что на фишках такой же величины выписаны буквы из слов, составляющих определенную фразу. В начальном положении фишки с буквами расположены в вершинах графа так, что если обходить вершины в порядке возрастания номеров, то получим последовательность букв в фразе, а вершина с наибольшим номером останется свободной. Предположим, что фишки

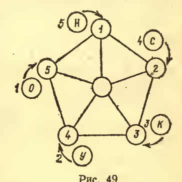


Рис. 49

в случайном порядке расставлены в вершинах графа. Цель игры заключается в том, чтобы, передвигая фишки вдоль ребер графа на свободное место, разместить их в первоначальном порядке, т. е. так, чтобы они образовали выбранную фразу при обходе вершин графа в порядке возрастания их номеров. Конечно, игры такого типа представляют интерес не при всех графах. Одним из естественных условий, скажем, является то, что граф должен быть связным. Если граф уже выбран, то можно исследовать, от каких случайных расположений фишек можно перейти к первоначальному, как фактически осуществить такой переход, как сделать его за наименьшее возможное число ходов и т. п. Следует отметить, что если характеризовать всевозможные случайные расположения фишек перестановками множества номеров вершин графа (т. е. считать, что фишки занумерованы теми же чис-

лами, что и вершины графа кроме последней), то всем «допустимым» расположениям фишек — таким, от которых можно перейти к первоначальному, — будут соответствовать перестановки, образующие группу (почему?). А различным «ходам» будут отвечать умножения на определенные перестановки из этой группы, которые являются ее системой образующих (почему?).

2. Игра «домино». Эта игра построена по образцу кубика Рубика. Прямоугольный параллелепипед составлен из 18 маленьких кубиков, образующих две квадратные плиты по 9 кубиков в каждой (рис. 50). Кубики скреплены так, что плиты могут свободно вращаться одна относительно другой (рис. 50). Кроме того, могут вращаться и прямоугольные плиты, состоящие из 6 кубиков. Три таких плиты параллельны одной паре боковых (не квадратных) граней и три — другой. Параллелепипед совмещается сам с собой при вращениях квадратных плит

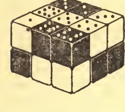



Рис. 50

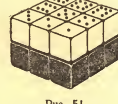
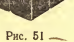



Рис. 51

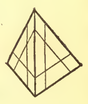


Рис. 52

на углы $\pi/2$, π, $3\pi/2$ и неквадратных плит — на угол π. После осуществления любого из вращений, при которых параллелепипед самосовмещается, снова можно выполнять произвольное вращение. Маленькие кубики, из которых составлен параллелепипед, двух цветов — белого и черного, по 9 каждого цвета. На кубиках нанесены кружочки как на костяшках домино. На белых кубиках эти кружочки черные, а на черных — белые. Имеется по одному белому и черному кубику с одним кружочком, по одному — с двумя, с тремя и т. д. до девяти.

В начальном положении квадратные плиты составлены из кубиков одинакового цвета, которые расположены в порядке возрастания числа кружочков справа налево и снизу вверх (рис. 51). Кубики черной и белой плит с одинаковым числом кружочков расположены один под другим. После случайных вращений параллелепипед при-

обретает пеструю окраску и нарушается порядок расположения кубиков внутри каждой из плит (по числу кружочков) и из разных плит. Требуется путем выполнения ряда последовательных вращений привести параллелепипед в первоначальное состояние.

Алгоритмы, переводящие параллелепипед «домино» в исходное состояние, вначале располагают на своих местах угловые кубики, а затем — кубики середин граней. Отметим, что при анализе этой игры нельзя считать серединные кубики неподвижными — то, что разрешается вращать стоящие посередине прямоугольные плиты, в случае «домино» существенно. Группа перестановок, связанная с вращениями «домино», состоит из

$$(4!\ 8!)\ 8!/2 = 2^{16}\ 3^5\ 5^2\ 7^2 \approx 1{,}95 \cdot 10^{10}$$

элементов!

Обобщением игры «домино и кубика Рубика является «волшебный параллелепипед». Имеется в виду параллелепипед, разбитый на $n \times m \times k$ маленьких кубиков плоскостями, параллельными его граням. Неквадратные грани можно поворачивать только на 180°. Внутренние плиты тоже вращаются. Понятно, что анализ этого общего случая основывается на тех же идеях, однако чисто технически все сложнее.

Недавно в Венгрии налажен выпуск $4 \times 4 \times 4$ кубиков, называемых «Месть Рубика»!

3. Волшебный тетраэдр. Тетраэдр разбит плоскостями на части так, как показано на рис. 52. Части, находящиеся в центрах граней, можно считать неподвижными. При поворотах граней перемещается 4 угловых и 6 реберных элементов, форму которых читатель легко себе представит на основании рис. 52. В начальном положении каждая грань тетраэдра окрашена в один из четырех цветов. Цель игры прежняя — как перейти к начальному расположению частей, получив в руки «пестрый» тетраэдр.

Группа перестановок, связанная с тетраэдром, состоит из

$$(4!/2)\ (6!/2)\ (2^6/2)\ (3^4/3) = 2^{10}3^6 5 = 3\ 732\ 480$$

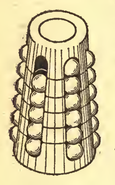
элементов.

Аналогичные игры можно образовывать и для других правильных многогранников, например для додекаэдра. Группа перестановок, получающаяся при рассмотрении игры, связанной с додекаэдром, состоит из

$$(30!/2)\ (20!/2)\ (20^{30}/2)\ (3^{20}/3) \approx 1{,}01 \cdot 10^{68}$$

элементов. Это очень большая группа, и поэтому цепочка преобразований, которые необходимо провести, чтобы из заданного положения «волшебного» додекаэдра перейти к начальному, будет, вообще говоря, длинной. Трудно ожидать, что «волшебный додекаэдр» получит столь широкое распространение, как «волшебный куб».

4. Волшебная пирамидка. Основой этой игрушки является урезанный конус, разбитый плоскостями, параллельными основанию, на 6 частей, которые крепятся на общей оси, совпадающей с осью симметрии конуса, и могут свободно вокруг нее вращаться. В этих частях сделано 6 вертикальных прорезей, в которых крепятся шарики одинакового диаметра. Прорези устроены так, что шарики из них не выкатываются. Шарики окрашены в 6 цветов по числу прорезей. Шарики одного цвета имеют разную тональность — от более светлых до более темных тонов. Имеется 6 шариков каждого цвета, кроме одного цвета, в который окрашено на один шарик меньше, так что одно из 36 мест для шариков в прорезях остается свободным. Кроме того, в одной прорези имеется внутренняя кнопка, позволяющая «утапливать» шарик, стоящий на этом месте, и ставить на его место другой шарик. «Утопленный» шарик возвращается на свое место как только оно освобождается. Общий вид волшебной пирамидки изображен на рис. 53; пирамидкой она называется потому, что конус, после того как в нем сделаны прорези, стал больше походить на пирамидку.


Рис. 53

В начальном положении шарики расположены в прорезях так, что в каждой из прорезей лежат упорядоченные по тональности шарики одного цвета, скажем снизу темнее, а чем выше, тем светлее. Случайными вращениями шести основных частей пирамидки вокруг оси приводят ее в «пестрое» положение. Требуется с помощью таких же вращений, перемещений шарика в одной из прорезей на свободное место, «утапливания» одного из шариков перевести пирамидку в начальное состояние. Игра эта интересная, однако она существенно проще игры «кубик Рубика».

В заключение отметим также, что югославский математик В. Чепулич в 1979 г. предложил перестановочную

модель для анализа шахматной игры. Построение такой модели требует довольно длинных выкладок, и пока неясно, может ли она применяться в шахматной теории. Поэтому, хотя сама модель достаточно занимательна, мы ее описывать здесь не будем.

Упражнения

1. Неориентированный граф называется *полным*, если любые две его вершины соединены ребром. Рассмотреть игру типа «хамелеон» для полного графа. В частности, установить, можно ли от любого расположения фишек в вершинах такого графа перейти к начальному расположению? Если это так, то какое наибольшее число ходов необходимо осуществить для перехода к начальному расположению фишек в случае полных графов с тремя, четырьмя, пятью вершинами?

2. Построить неориентированный граф с шестнадцатью вершинами, перестановочная игра на котором совпадала бы с игрой «в пятнадцать».

3. Доказать, что группа перестановок, получаемых при вращениях «домино», состоит из $(4!\,8!)8!/2$ перестановок.

4. Какие перестановочные конструкции используются при построении группы перестановок для «домино».

5. Разработать алгоритм, позволяющий от любого допустимого расположения кубиков в «домино» перейти к начальному.

6. Проверить, что группа перестановок, получаемых при вращениях «волшебного тетраэдра», состоит из $(4!/2)\,(6!/2)\,(2^6/2)\,(3^4/3)$ элементов.

7. Можно ли от любого расположения шариков в волшебной пирамидке перейти к начальному?

ОТВЕТЫ, УКАЗАНИЯ, РЕШЕНИЯ

§ 1

1. а) $(f \circ g)(x) = 6x + 13$, $(g \circ f)(x) = 6x + 11$;
б) $(f \circ g)(x) = x^6 + 10x^5 + 25x^4 + 3$, $(g \circ f)(x) = x^6 + 14x^4 + 57x^2 + 72$;
в) $(f \circ g)(x) = x^6 + 6x^4 + 13x^2 + 11$, $(g \circ f) = x^6 + 2x^4 + 2x^3 + x^2 + x + 3$.

$$\text{г) } (f \circ g)(x) = \begin{cases} \dfrac{14x+11}{1-x}, & \text{если } x \neq -\dfrac{3}{2},\ x \neq 1, \\ \text{не определена}, & \text{если } x = -\dfrac{3}{2} \text{ или } x = 1; \end{cases}$$

$$(g \circ f)(x) = \begin{cases} \dfrac{x+1}{x+2}, & \text{если } x \neq -2,\ x \neq 1, \\ \text{не определена}, & \text{если } x = -2 \text{ или } x = 1. \end{cases}$$

2. а) Замкнуто; б) замкнуто; в) замкнуто; д) незамкнуто.

§ 2

2. При $m \leqslant n$ существует $n(n-1)\ldots(n-m+1)$ разных инъекций множества A в множество B.

3. Решение. Пусть B есть n-элементное множество. Зафиксируем произвольное множество A, $|A| = m$. Образ множества A при любом инъективном отображении $A \to B$ будет некоторым m-элементным подмножеством множества B. Множество A будет иметь тот же самый образ $A' \subset B$ при разных инъекциях тогда и только тогда, когда они будут отличаться на некоторую биекцию множества A в себя. Поскольку $|A'| = |A| = m$, то существует $m!$ различных биекций A на себя. А поэтому есть $C_n^m = \dfrac{n(n-1)\ldots(n-m+1)}{m!}$ различных m-элементных подмножеств множества B.

5. На каждой вертикальной или горизонтальной прямой графика биекции отмечена одна и только одна вершина сетки. При стрелочном изображении биекции $A \to B$ из каждой точки, которой обозначен элемент множества A, выходит точно одна стрелка и в каждую точку, которая является обозначением элемента множества B, входит одна и только одна стрелка.

6. 44. Указание. Сначала нужно найти количество перестановок, которые оставляют без изменения по меньшей мере один элемент множества M. 7. $6 \cdot 7^5$.

8. Пусть G_1 и G_2 — множества перестановок φ, которые удовлетворяют соответственно условиям $(1)\varphi - (2)\varphi > 0$ и $(1)\varphi - (2)\varphi < 0$. Понятно, что каждая перестановка содержится в одном из этих множеств. Поскольку отображение множества G_1 на множество G_2,

в соответствии с которым каждой перестановке

$$\varphi=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ i_1 & i_2 & i_3 & \dots & i_n\end{pmatrix}$$

из множества G_1 ставится в соответствие перестановка

$$\varphi'=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ i_2 & i_1 & i_3 & \dots & i_n\end{pmatrix}$$

из множества G_2, биективно (проверьте), то $|G_1|=|G_2|=n!/2$. Для $(n-1)!$ перестановки множества G_1 справедливо равенство $(1)\varphi-(2)\varphi=1$. Следовательно, существует $\frac{n!}{2}-(n-1)!$ перестановок, которые удовлетворяют условию упражнения.

§ 3

2. а) $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 1 & 2 & 1 & 1\end{pmatrix}$; б) $\begin{pmatrix}a & b & c & d & e\\ c & d & c & d & c\end{pmatrix}$;

в) $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 2 & 3 & 2 & 3\end{pmatrix}$.

4. Вершина (a, b) координатной сетки при построении графика преобразования $\varphi\circ\psi$ обозначается тогда и только тогда, когда существует такое число $c\in M$, что на графике преобразования φ обозначена вершина сетки (a, c), а на графике преобразования ψ — вершина (c, b).

5. Допустим сначала, что φ — не перестановка. Тогда найдутся элементы $a, b\in M$, $a\neq b$, такие, что $(a)\varphi=(b)\varphi$. Для них имеем $(a)(\varphi\circ\psi)=((a)\varphi)\psi=((b)\varphi)\psi=(b)(\varphi\circ\psi)$, что противоречит условию здачи. Если ψ — не перестановка, то множество образов элементов M при действии ψ является собственным подмножеством множества M. Следовательно, элементы вида $(a)(\varphi\circ\psi)=((a)\varphi)\psi$, $a\in M$, не исчерпывают все множество M, т. е. преобразование $\varphi\circ\psi$ — не сюръекция, а это противоречит условию задачи.

6. Указание. Воспользоваться утверждением, сформулированным в предыдущем упражнении.

7. а) $x=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 5 & 4 & 1 & 2 & 6 & 3\end{pmatrix}$; б) $x=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix}$.

8. а) Уравнение не имеет решений;

б) уравнение имеет четыре решения:

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 4 & 2\end{pmatrix},\quad \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 5 & 4 & 2\end{pmatrix},$$
$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 4 & 3\end{pmatrix},\quad \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 5 & 4 & 3\end{pmatrix};$$

в) уравнение не имеет решений;

г) уравнение имеет единственное решение $x=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 2 & 2 & 2\end{pmatrix}$.

§ 4

1. а) Нет; б) да; в) да.

2. а) Нет; б) да; в) да; г) ни одна из этих полугрупп группы не образует.

4. Таблица умножения абелевой группы симметрична относительно оси, которая проходит из левого верхнего ее угла к правому нижнему.

§ 5

1. Нет. Если граф задает преобразование, то из каждой его вершины выходит одна и только одна стрелка.

3. На графе произведения $\varphi \circ \psi$ преобразований φ, ψ множества M точки, которыми обозначены элементы $a, b \in M$, соединяются стрелкой в направлении от a к b тогда и только тогда, когда существует такая точка c, что на графе преобразования φ точки a, c соединяются стрелкой в направлении от a к c, а на графе преобразования ψ точки c, b соединены стрелкой в направлении от c к b.

§ 6

1. а) 12; б) 9. 2. 1, 2, 3, 4, 5, 6. 3. 30.

4. $(a_n, a_{n-1}, \ldots, a_2, a_1)$.

5. Указание. Рассмотреть перестановки

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

6. $\frac{8!}{3 \cdot 5}$. Указание. Воспользоваться решением упражнения 11, § 5.

9. Если перестановка φ имеет разложение

$$\varphi = \underbrace{(a_1, \ldots, a_s) \circ (b_1, \ldots, b_s) \circ \ldots \circ (c_1, \ldots, c_s)}_{l},$$

то цикл ψ определяется так:

$$\psi = (a_1, b_1, \ldots, c_1, a_2, b_2, \ldots, c_2, \ldots, a_s, b_s, \ldots, c_s).$$

Убедиться, что справедливо равенство $\psi^l = \varphi$.

§ 7

1. Указание. Доказательство легко проводится индукцией по числу n.

2. Достаточно проверить, что любое преобразование из $P(M)$ можно разложить в произведение перестановок из $S(M)$ и преобразования α. Это проверяется в несколько шагов:

а) умножением α справа или слева на подходящую перестановку можно получить всевозможные преобразования, переводящие какие-либо два элемента множества M в один и тот же его элемент;

б) из таких преобразований конструируются преобразования множества M, переводящие некоторые k элементов множества M в один и тот же элемент, а все остальные элементы оставляющие на месте ($k \leqslant |M|$);

в) очевидно, что любое преобразование из $P(M)$ является произведением преобразований вида б).

3. а) $(1, 3, 4, 7) = (1, 3) \circ (1, 4) \circ (1, 7) = (1, 2) \circ (4, 5) \circ (5, 6) \circ (6, 7) \circ (6, 5) \circ (5, 4) \circ (4, 3) \circ (3, 2) \circ (2, 1) = (1, 2) \circ (1, 2, 3, 4, 5, 6, 7)^{-3} \circ (1, 2) \circ (1, 2, 3, 4, 5, 6, 7)^{-1} \circ (1, 2) \circ (1, 2, 3, 4, 5, 6, 7)^{-1} \circ (1, 2) \circ (1, 2, 3, 4,$

5, 6, 7)$^{-1}\circ$(1, 2)$\circ$(1, 2, 3, 4, 5, 6, 7)$\circ$(1, 2)$\circ$(1, 2, 3, 4, 5, 6, 7)$\circ$ $\circ$(1, 2)$\circ$(1, 2, 3, 4, 5, 6, 7)$\circ$(1, 2)$\circ$(1, 2, 3, 4, 5, 6, 7)$\circ$(1, 2).

4. Сеть дорог можно рассматривать как граф с n вершинами. Наименьшее число связывающих дорог отвечает тому, что граф — дерево. Поэтому достаточно провести $n-1$ связывающих дорог.

8. n^{n-2}. **9.** Да. **10.** Да.

12. Из равенства $(i, j, k)=(i, j)\circ(i, k)$ вытекает, что $(i, j)= =(i, j, k)\circ(i, k)$. При фиксированных i, k получаем, что транспозиции вида (i, j) (i — фиксированный, j — произвольный) можно выразить через отмеченные перестановки. Осталось убедиться, что множество таких транспозиций является системой образующих S_n.

§ 8

1. Указание. Для произвольной перестановки $\alpha\in T$ существует натуральное число l, такое, что $\alpha^l=\varepsilon$ (например, равное порядку этой перестановки). Отсюда $\alpha^{-1}=\alpha^{l-1}$.

2. Группа S_4 содержит 4 трехэлементных подгруппы:

$$\{\varepsilon, (1, 2, 3), (1, 3, 2)\},\ \{\varepsilon, (1, 2, 4), (1, 4, 2)\},$$
$$\{\varepsilon, (1, 3, 4), (1, 4, 3)\},\ \{\varepsilon, (2, 3, 4), (2, 4, 3)\}.$$

3. Подгрупп второго порядка в S_5 столько, сколько имеется перестановок из S_5 порядка 2. Перестановка имеет порядок 2 тогда и только тогда, когда она является транспозицией или произведением двух взаимно простых транспозиций. Следовательно, таких перестановок $C_5^2+C_5^2\cdot C_3^2=40$.

4. Четверная группа Клейна содержит 3 нетривиальные собственные подгруппы — любой ее неединичный элемент вместе с тождественной подстановкой образует подгруппу. Циклическая группа C_4 содержит одну нетривиальную собственную подгруппу, а C_5 не содержит нетривиальных собственных подгрупп.

8. Центр S_4 совпадает с тривиальной подгруппой $\{\varepsilon\}$. Центр C_n совпадает с C_n.

9. 2, 3, 4, 5, 6. **10.** 30.

§ 9

1. Проверить, что вращение α правильного n-угольника вокруг центра на угол $2\pi/n$ и симметрия β относительно любой из осей не коммутируют, т. е. $\alpha\circ\beta\neq\beta\circ\alpha$.

2. В группе D_7 имеются (без учета ε) лишь элементы порядка 7 (неединичные вращения) и элементы порядка 2 (симметрии). В группе D_8 среди вращений имеются: один элемент порядка 2 (угол π), два элемента порядка 4 (углы $\pi/2$, $3\pi/2$), 4 элемента порядка 8.

3. Системы образующих группы D_n из двух элементов порядка 2 существуют. Такими будут, например, симметрии относительно осей, образующих угол $2\pi/n$. Они, очевидно, неприводимы. Неприводимые системы образующих D_n, состоящие из разного количества перестановок, существуют, когда n — непростое число.

5. Да.

8. Центр группы вращений тетраэдра — тривиальная подгруппа.

10. Группа симметрий прямой призмы, в основании которой лежит правильный n-угольник, — это группа D_n, одинаково действующая на множествах вершин верхнего и нижнего оснований, а ее группа вращений — подгруппа D_n, совпадающая с C_n.

§ 10

1. Если $|G_1|=|G_2|=2$, то группы $G_1=\{e_1, g_1\}$ и $G_2=\{e_2, g_2\}$ — циклические и соответствие $e_1 \leftrightarrow e_2$, $g_1 \leftrightarrow g_2$ является изоморфизмом этих групп. Если $|G_1|=|G_2|=3$, то группы $G_1=\{e_1, g_1, h_1\}$, $G_2=\{e_2, g_2, h_2\}$ тоже являются циклическими и любое из соответствий

$$e_1 \leftrightarrow e_2, \quad g_1 \leftrightarrow g_2, \quad h_1 \leftrightarrow h_2$$

либо

$$e_1 \leftrightarrow e_2, \quad g_1 \leftrightarrow h_2, \quad h_1 \leftrightarrow g_2$$

является изоморфизмом этих групп.

2. Указание. Установить сначала, что в группе, состоящей из четырех элементов, могут встречаться лишь элементы порядков 2 и 4. Затем рассмотреть возможные случаи.

4. Стабилизатор любого элемента регулярной группы перестановок является тривиальной подгруппой.

7. Указание. Проверить, что композиция изоморфизмов, т. е. их последовательное осуществление, тоже изоморфизм.

§ 11

1. Разложения S_3 на правые и левые классы смежности по подгруппе B совпадают. Это строки из

ε	$(1, 2, 3)$	$(1, 3, 2)$
$(1, 2)$	$(1, 3)$	$(2, 3)$.

Разложением S_3 на правые классы смежности по подгруппе A будут строки из

ε	$(1, 2)$
$(1, 3)$	$(1, 2, 3)$
$(2, 3)$	$(1, 3, 2)$

а на левые — строки из

ε	$(1, 2)$
$(1, 3)$	$(1, 3, 2)$
$(2, 3)$	$(1, 2, 3)$

3. Если H — подгруппа индекса 2 в группе G, то множество $G \mid H$ является одним из двух классов смежности (как правым, так и левым).

4. Указание. Убедиться, что в S_m есть подгруппа такого порядка.

5. 1, 2, 3, 4, 6, 12. В группе D_{12} существуют перестановки порядков 2, 3, 6 (без учета тождественной перестановки).

6. 1, 2, 3, 4, 6, 8, 12, 24. В группе S_4 существуют элементы порядков 2, 3, 4 (без учета тождественной перестановки).

§ 12

1. Стабилизатор вершины в группе G состоит из трех вращений куба вокруг диагонали (на углы 0, $2\pi/3$, $4\pi/3$ по часовой стрелке).

3. а) Очевидно, имеем $\varepsilon^{-1} \circ \alpha \circ \varepsilon = \alpha$; б) если $\gamma^{-1} \circ \alpha \circ \gamma = \beta$, то $(\gamma^{-1})^{-1} \circ \beta \circ \gamma^{-1} = \alpha$; в) если $\gamma^{-1} \circ \alpha \circ \gamma = \beta$ и $\delta^{-1} \circ \beta \circ \delta = \pi$, то $(\gamma \circ \delta)^{-1} \circ \alpha \circ (\gamma \circ \delta) = \pi$.

4. Если перестановки α, β сопряжены с перестановкой γ, то они сопряжены между собой. Поэтому множество G разбивается на нан-

большие возможные подмножества попарно сопряженных между собой перестановок. Пусть R_1, R_2 — два таких подмножества, причем $R_1 \cap R_2 \neq \varnothing$. Тогда найдется такая перестановка α, что $\alpha \in R_1$ и $\alpha \in R_2$. Она сопряжена со всеми элементами из R_1 и со всеми элементами из R_2. Отсюда получаем, что все элементы $R_1 \cup R_2$ между собой попарно сопряжены. А это противоречит выбору R_1, R_2. Следовательно, $R_1 \cap R_2 = \varnothing$.

5. Указание. Можно воспользоваться решением задачи 7.

7. Указание. Воспользоваться тем, что сопряженная перестановка к циклу тоже цикл:

$$\begin{pmatrix} 1 & 2 & \dots & k \\ i_1 & i_2 & \dots & i_k \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & \dots & k-1 & k \\ 2 & 3 & \dots & k & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & k \\ i_1 & i_2 & \dots & i_k \end{pmatrix} = (i_1, i_2, \dots, i_k),$$

а сопряженная с произведением взаимно простых перестановок совпадает с произведением сопряженных к каждой из них.

10. Проверить, что существуют перестановки, переводящие данную грань в любую другую. Стабилизатор грани совпадает с группой вращений куба вокруг оси, проходящей через центр грани и ей перпендикулярной.

§ 14

2. Группой инерции многочлена $f(x_1, x_2, x_3, x_4)$ является циклическая группа порядка 2: $\{\varepsilon, (2, 4)\}$.

3. Группа инерции многочлена $A(x_1, x_2, x_3, x_4)$ состоит из 12 перестановок.

4. Доказательство. Рассмотрим многочлен $f(x_1, x_2, \dots, x_n) = x_1 + 2x_2 + \dots + nx_n$. Его группа инерции тривиальна. Кроме того, для каждой перестановки $\sigma \in S_n$, $\sigma \neq \varepsilon$ имеем $f^\sigma \neq f$. А поэтому для произвольной подгруппы $G = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$ группы S_n многочлен $f^{\alpha_1} f^{\alpha_2} \dots f^{\alpha_k} = h(x_1, x_2, \dots, x_n)$ инвариантен относительно действия тех и только тех перестановок, которые входят в подгруппу G.

5. $o_4(x_1^2 x_2 x_3^2 x_4)$ содержит шесть одночленов.

7. $o_n(x_1 x_2 \dots x_l)$, $l \leqslant n$, содержит $C_n^l = \dfrac{n!}{l!\,(n-l)!}$ одночленов.

§ 15

2. 5. 4. Подгруппа, которая содержит три элемента.

5. Центром группы A_n является тривиальная подгруппа ($n > 3$). Указание. Доказать, что каждая четная перестановка, которая коммутирует со всеми циклами длины 3, тождественная.

7. Указание. Воспользоваться равенствами $(i, j, k) = (i, j) \circ (i, k)$, $(i, j) \circ (k, l) = (i, l, k) \circ (i, j, k)$, где i, j, l, k — разные элементы множества $\{1, 2, \dots, n\}$.

8. Да.

9. Указание. Доказать, что при умножении перестановки на транспозицию четность числа инверсий ее второго ряда изменяется.

10. Указание. Воспользоваться тем, что число T_n^k перестановок множества из n элементов, вторые ряды которых содержат ровно k инверсий, удовлетворяет соотношению

$$T_n^k = T_{n-1}^k + T_{n-1}^{k-1} + \dots + T_{n-1}^{k-n+1},$$

где $T_n^j = 0$ для $j < 0$ или $j > \dfrac{n-1}{2}$.

11. **Указание.** Разложить каждый цикл в циклической форме записи перестановки в произведение транспозиций и подсчитать число транспозиций.

§ 16

1. а) $s_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$; б) $s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$; в) $o_3(x_1^2x_2) = \sigma_1\sigma_2 - 3\sigma_3$.

2. а) $\{(4;\ 16),\ (16;\ 4)\}$; б) $\{(2;\ 3),\ (3;\ 2),\ (2;\ -5),\ (-5;\ 2)\}$; в) $\{(1;\ 3),\ (3;\ 1)\}$.

3. **Указание.** Выразить сумму попарных произведений длин сторон треугольника и произведение длин всех его сторон через данные числа и воспользоваться тем, что в формуле Герона под знаком корня стоит симметрический многочлен.

4. **Указание.** Для многочлена $f(x_1, x_2)$ рассмотрите одночлен $ax_1^kx_2^l$, у которого показатель степени k наивысший. Если таких одночленов несколько, то нужно взять тот, у которого показатель l наивысший. Докажите, что одночлен с такими свойствами не может уничтожаться при переходе от $f(x_1, x_2)$ к $f(x_1+x_2, x_1x_2)$.

6. Действительно, если в многочлене $f(x_1, x_2)$ поменять местами x_1 и x_1, то он, с одной стороны, не изменится, а с другой — изменит знак на противоположный. Значит, $f(x_1, x_1) = -f(x_1, x_1)$, т. е. $f(x_1, x_1)$ тождественно равно 0.

8. **Указание.** Докажите, что $f(x_1, x_2, x_3) = 4\max(x_1, x_2, x_3)$.

§ 17

2. Разделим многочлен $f(x)$ на $x-\alpha$ с остатком, т. е. запишем равенство $f(x) = (x-\alpha)g(x)+r$, где r — некоторое число. Подставляя в это равенство вместо переменной x число α, получим верное числовое равенство: $f(\alpha) = (\alpha-\alpha)g(\alpha)+r$. Отсюда $r = f(\alpha) = 0$.

3. **Указание.** Согласно упражнению 2 многочлен $f(x)$ раскладывается в произведение $f(x) = (x-\xi_1)(x-\xi_2)\ldots(x-\xi_n)$. Раскрывая скобки в этом произведении и приравнивая коэффициенты при одинаковых степенях x в правой и левой части после раскрытия скобок, получим требуемое.

4. **Указание.** Воспользоваться основной теоремой § 16.

5. Числовое поле образуют все действительные числа, все числа вида $a+b\sqrt{p}$, где p — простое число, и многие другие числовые множества. Однако, любое числовое поле содержит поле рациональных чисел $\mathbf{Q}$ (поскольку оно должно содержать 0 и 1). Всевозможные числа вида $a+b\sqrt{3}$ образуют числовое поле, поскольку сумма и разность чисел такого вида снова будет числом такого вида:

$$(a+b\sqrt{3}) \pm (c+d\sqrt{3}) = (a \pm c)+(b \pm d)\sqrt{3}.$$

Для произведения и частного чисел такого вида имеем

$$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\sqrt{3},$$

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}} = \frac{(a+b\sqrt{3})(c-d\sqrt{3})}{c^2-3d^2} = \frac{ac-3bd}{c^2-3d^2}+\frac{bc-ad}{c^2-3d^2}\sqrt{3},$$

где $c+d\sqrt{3} \neq 0$. То есть это числа такого же вида, и, следовательно, множество таких чисел образует поле.

§ 18

4. а) Да; б) нет.

5. Указание. На каждой фишке напишем новый номер по следующему правилу. Если старый номер 14 (15), то новый 15 (соответственно 14). На всех остальных фишках новый номер совпадает со старым. Сами же фишки передвигать не будем. Размещение фишек с новыми номерами характеризуется четной перестановкой и поэтому от него можно перейти к стандартному относительно новых (!) номеров. Но стандартное размещение относительно новых номеров — это требуемое размещение относительно старых номеров.

6. Указание. Занумеровать буквы в том порядке, в котором они стоят в фразе «игра в пятнадцать». Учесть, что среди этих букв есть одинаковые — буква «а», и воспользоваться решением предыдущего упражнения.

§ 19

2. $\langle k_1, k_2, \ldots, k_s, l_1, l_2, \ldots, l_t \rangle$.

4. $\alpha\times\beta =$

$$= \begin{pmatrix} (1, 1) & (1, 2) & (1, 3) & (2, 1) & (2, 2) & (2, 3) & (3, 1) & (3, 2) & (3, 3) \\ (2, 3) & (2, 2) & (2, 1) & (3, 3) & (3, 2) & (3, 1) & (1, 3) & (1, 2) & (1, 1) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 4 & 9 & 8 & 7 & 3 & 2 & 1 \end{pmatrix}.$$

5. Пор. $(\alpha\times\beta) = K$ (пор. α, пор. β)

6.

$$K = \{\varepsilon, (1, 2)\} \oplus \{\varepsilon, (3, 4)\},$$
$$L = \{\varepsilon, (1, 2)\} \times \{\varepsilon, (1, 2)\};$$

при рассмотрении перестановок из L нужно учесть естественную нумерацию элементов множества $\{1, 2\}\times\{1, 2\}$.

7. $(\alpha\oplus\beta)^{-1} = \alpha^{-1}\oplus\beta^{-1}$, $(\alpha\times\beta)^{-1} = \alpha^{-1}\times\beta^{-1}$.

9. $[\alpha, \beta_1, \beta_2, \ldots, \beta_k]^{-1} = [\alpha^{-1}; \beta^{-1}_{(1)\alpha^{-1}}, \beta^{-1}_{(2)\alpha^{-1}}, \ldots, \beta^{-1}_{(k)\alpha^{-1}}]$.

11. Группа симметрий многочлена f является сплетением $S_2 \wr S_3$, для которого естественным образом определено действие на множестве $\{1, 2, 3, 4, 5, 6\}$ номеров кортежей из $\{1, 2\}\times\{1, 2, 3\}$.

§ 20

1. а) Меняются местами средние кубики (фв, фи) и (пв, пн); б) меняются местами угловые кубики (флв, фвп), (пит, фип).

2. Обе перестановки имеют порядок 6.

6. Прямые суммы $\alpha\oplus\beta$ перестановок $\alpha\in S_8$, $\beta\in S_{12}$, таких, что $\alpha\oplus\beta$, — четная перестановка (т. е. α и β имеют одинаковую четность).

7. Проверить, что имеет место равенство $(i, j, k) = ((i, j)(j, k))^2$.

8. Коммутант S_n совпадает с A_n. Указание. Воспользоваться решением предыдущей задачи.

10. Можно.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Подробное обсуждение понятий отображения и преобразования можно найти в книгах:

Кемени Дж., Снелл Дж., Томпсон Дж. Введение в конечную математику. — М.: Мир, 1965.

Сойер У. Путь в современную математику. — М.: Мир, 1972.

Фрейденталь Г. Математика в науке и вокруг нас. — М.: Мир, 1977.

Коксетер Г. С. М., Грейтцер С. Л. Новые встречи с геометрией. — М.: Наука, 1978.

В последних двух книгах изучаются геометрические преобразования. Много комбинаторных задач, связанных с понятием преобразования и перестановки, есть в книгах:

Ежов И. И., Скороход А. В., Ядренко М. И. Элементы комбинаторики. — М.: Наука, 1977.

Виленкин Н. Я. Популярная комбинаторика. — М.: Наука, 1975.

Калбертсон Дж. Математика и логика цифровых устройств. — М.: Просвещение, 1965.

Гик Е. Я. Математика на шахматной доске. — М.: Наука, 1976.

Реньи А. Трилогия о математике. — М.: Мир, 1980.

Подробнее ознакомиться с теоретико-групповыми понятиями можно в следующих книгах:

Гроссман И., Магнус В. Группы и графы. — М.: Мир, 1971.

Александров П. С. Введение в теорию групп. — М.: Наука, 1980.

Фрид Э. Элементарное введение в абстрактную алгебру. — М.: Мир, 1979.

Изучению явлений симметрии в различных разделах естествознания посвящены книги:

Дмитриев И. С. Симметрия в мире молекул. — Л.: Химия, 1976.

Красилов В. Б. О симметрии в биологии. — Л.: Наука, 1971.

Вейль Г. Симметрия. — М.: Наука, 1968.

Узоры симметрии: Сб. переводов/Под ред. акад. Н. В. Белова и проф. Н. Н. Шефтала. — М.: Мир, 1980.

Шаскольская М. П. Очерки о свойствах кристаллов. — М.: Наука, 1985.

Компанеец А. С. Симметрия в микро- и макромире. — М.: Наука, 1978.

Болтянский В. Г., Виленкин Н. Я. Симметрия в алгебре. — М.: Наука, 1967.

Варга Б., Димень Ю., Лопариу Э. Язык, музыка, математика. — М.: Мир, 1981.

Для ознакомления с теорией Галуа отсылаем читателя к книгам:

Постников М. М. Основы теории Галуа. — М.: Физматгиз, 1960.

Артин Э. Теория Галуа. — Киев: Радянська школа, 1963.

Алексеев В. Б. Теорема Абеля в задачах и решениях. — М.: Наука, 1976.

Более глубокие сведения по теории групп, теории многочленов, комбинаторике читатель может почерпнуть из книг:

Кострикин А. И. Введение в алгебру. — М.: Наука, 1977.

Калужнин Л. А. Введение в общую алгебру. — М.: Наука, 1973.

Ван дер Варден Б. Л. Алгебра. — М.: Наука, 1979.

Скачков В. Н. Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982.

СОДЕРЖАНИЕ


55 коп.